KOREAN PATENT ABSTRACT (KR)

PUBLICATION

(51) IPC Code: G06F 17/00
(11) Publication No.: P2003-0007773 (43) Publication Date: 23 January 2003
(21) Application No.: 10-2001-7016266 (22) Application Date: 29 November 2002
(86) International Application No.: PCT/JP2002/02956
(86) International Application Date: 27 March 2002
(87) International Publication No.: WO 2002/80442
(87) International Publication Date: 10 October 2002

(71) Applicant:
SONY CORPORATION

(72) Inventor:
ISHIGURO, Ryuji

(54) Title of the Invention:

INFORMATION PROCESSING APPARATUS

Abstract:

An information processing apparatus capable of management of copyright in the SDMI and management of copyright of a content transferred via the Internet. A content encrypted by a content key (Kc) into data (Enc (Kc, Content)) is recorded. Simultaneously with this, a header (Header), a certificate (Cert), data Enc (KR, Kc) created by encrypting the content key (Kc) by a root key (KR), and an enabling key block (EKB) are recorded. The header contains a content ID (CID), a license ID (LID), an URL, and a watermark (WM). Furthermore, a header signature (Sig (Header)) is added. This invention can be applied to an apparatus providing a content.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
G06F 17/00

(11) 공개번호 특2003-0007773
(43) 공개일자 2003년01월23일

(21) 출원번호 10-2002-7016266
(22) 출원일자 2002년11월29일
번역문 제출일자 2002년11월29일
(86) 국제출원번호 PCT/JP2002/02956
(86) 국제출원출원일자 2002년03월27일
(87) 국제공개번호 WO 2002/80442
(87) 국제공개일자 2002년10월10일

(81) 지정국 국내특허 : 대한민국, 미국, 일본,
EP 유럽특허: 오스트리아, 벨기에, 스위스, 독일, 덴마크, 스페인, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴, 핀랜드, 사이프러스, 터어키,

(30) 우선권주장 JP-P-2001-00094807 2001년03월29일 일본(JP)

(71) 출원인 소니 가부시끼 가이샤
일본국 도쿄도 시나가와쿠 키타시나가와 6쵸메 7반 35고

(72) 발명자 이시구로,류지
일본141-0001도쿄도시나가와꾸기따시나가와6쪼메7-35소니가부시끼가이샤내

(74) 대리인 주성민
구영창

심사청구 : 없음

(54) 정보 처리 장치

요약

본 발명은, SDMI에서의 저작권 관리와, 인터넷을 통해 전송되는 콘텐츠의 저작권을 관리할 수 있도록 한 정보 처리 장치에 관한 것이다. 콘텐츠를 콘텐츠 키 Kc로 암호화한 데이터 Enc(Kc, Content)가 기록됨과 함께, 헤더(Header), 증명서(Cert), 콘텐츠 키 Kc를 루트 키 KR로 암호화한 데이터 Enc(KR, Kc), 및 유효화 키 블록(EKB)이 기록된다. 헤더에는, 콘텐츠 ID (CID), 라이센스 ID(LID), URL, 및 워터마크(WM)가 포함된다. 또한, 헤더의 서명 Sig(Header)이 부가된다. 본 발명은, 콘텐츠를 제공하는 장치에 적용할 수 있다.

대표도

도 25

색인어
정보 처리 장치, 콘텐츠, 디바이스, 라이센스, 클라이언트, 노드, 리프

명세서

기술분야

본 발명은, 정보 처리 장치에 관한 것으로, 특히, 다른 시스템에서, 동일한 포맷으로 콘텐츠를 관리할 수 있도록 한, 정보 처리 장치에 관한 것이다.

배경기술

최근, 인터넷으로 대표되는 네트워크가 보급되어, 오디오나 비디오 등의 각종의 콘텐츠가, 인터넷을 통해 전송되는 경우가 많아지게 되었다.

인터넷은, 그 규모가 세계적이기 때문에, 부정하게 복사된 콘텐츠가 인터넷을 통해 배포되면, 그 콘텐츠의 저작권자가 입는 피해는, 상당히 커지게 된다.

또한, 오디오 장치에서, 사용자가, 음악 정보 등을 복사하여 이용하는 경우 에서의 저작권을 관리하는 시스템으로서, SDMI(Secure Digital Music Intiative)이 존재하며, 이 SDMI의 규정에 기초하여, 콘텐츠의 저작권이 관리되도록 이루어져 있다.

그러나, 사용자가, 오디오 장치를 이용하여 콘텐츠를 복사하고, 이용하는 경우에서의 저작권 관리와, 인터넷을 통해 배포되는 콘텐츠의 저작권을 관리하는 경우에서는, 그 전송 형태가 다르기 때문에, 각각 독자의 저작권 관리를 위한 포맷이 필요해진다.

그 결과, 사용자 혹은 콘텐츠를 이용하는 장치의 메이커는, 그 장치를 어떠한 시스템에 대해서도 적용할 수 있도록 하기 위해서는, 각각, 전용의 포맷으로 데이터를 수수할 수 있도록 구성할 필요가 있었다.

그 결과, 특히, 인터넷을 통해 배포되는 콘텐츠의 저작권을 관리하는 것이 곤란하게 된다는 과제가 있었다.

발명의 상세한 설명

본 발명은, 이러한 상황을 감안하여 이루어진 것으로, 다른 시스템에서도, 확실하게 저작권을 관리할 수 있도록 하는 것이다.

본 발명의 제1 정보 처리 장치는, 콘텐츠를 취득하는 콘텐츠 취득 수단과, 콘텐츠 취득 수단에 의해 취득된 콘텐츠에 부가되어 있는 워터마크를 추출하는 추출 수단과, 추출 수단에 의해 추출된 워터마크를 포함하는 헤더를 작성하는 헤더 작성 수단과, 비밀 키를 이용하여, 헤더 작성 수단에 의해 작성된 헤더의 데이터에 기초한 디지털 서명을 작성하는 디지털 서명 작성 수단과, 콘텐츠 취득 수단에 의해 취득된 콘텐츠를 암호화하는 암호화 수단과, 암호화 수단에 의해 암호화된 콘텐츠를 복호하는 데 필요한 키 정보를 포함하는 키 정보를 취득하는 키 정보 취득 수단과, 헤더 작성 수단에 의해 작성된 헤더, 디지털 서명 작성 수단에 의해 작성된 디지털 서명, 암호화 수단에 의해 암호화된 콘텐츠, 및 키 정보 취득 수단에 의해 취득된 키 정보를, 파일 포맷으로 포맷화하여, 출력하는 포맷화 수단을 포함하는 것을 특징으로 한다.

상기 워터마크는, 복사 관리 정보를 포함하도록 할 수 있다.

상기 헤더 작성 수단에 의해 작성된 헤더는, 콘텐츠를 식별하는 콘텐츠 식별 정보, 및 콘텐츠의 라이센스를 특정하는 라이센스 특정 정보를 더 포함하도록 할 수 있다.

상기 비밀 키에 대응하는 공개 키를 포함하는 증명서를 취득하는 증명서 취득 수단을 더 포함하며, 포맷화 수단은, 또한, 증명서 취득 수단에 의해 취득된 증명서를, 파일 포맷으로 포맷화하여, 출력하도록 할 수 있다.

본 발명의 제1 정보 처리 방법은, 콘텐츠를 취득하는 콘텐츠 취득 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는 워터마크를 추출하는 추출 단계와, 추출 단계의 처리에 의해 추출된 워터마크를 포함하는 헤더를 작성하는 헤더 작성 단계와, 비밀 키를 이용하여, 헤더 작성 단계의 처리에 의해 작성된 헤더의 데이터에 기초한 디지털 서명을 작성하는 디지털 서명 작성 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠를 암호화하는 암호화 단계와, 암호화 단계의 처리에 의해 암호화된 콘텐츠를 복호하는 데 필요한 키 정보를 포함하는 키 정보를 취득하는 키 정보 취득 단계와, 헤더 작성 단계의 처리에 의해 작성된 헤더, 디지털 서명 작성 단계의 처리에 의해 작성된 디지털 서명, 암호화 단계의 처리에 의해 암호화된 콘텐츠, 및 키 정보 취득 단계의 처리에 의해 취득된 키 정보를, 파일 포맷으로 포맷화하고, 출력하는 포맷화 단계를 포함하는 것을 특징으로 한다.

본 발명의 제1 기록 매체의 프로그램은, 콘텐츠를 취득하는 콘텐츠 취득 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는 워터마크를 추출하는 추출 단계와, 추출 단계의 처리에 의해 추출된 워터마크를 포함하는 헤더를 작성하는 헤더 작성 단계와, 비밀 키를 이용하여, 헤더 작성 단계의 처리에 의해 작성된 헤더의 데이터에 기초한 디지털 서명을 작성하는 디지털 서명 작성 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠를 암호화하는 암호화 단계와, 암호화 단계의 처리에 의해 암호화된 콘텐츠를 복호하는 데 필요한 키 정보를 포함하는 키 정보를 취득하는 키 정보 취득 단계와, 헤더 작성 단계의 처리에 의해 작성된 헤더, 디지털 서명 작성 단계의 처리에 의해 작성된 디지털 서명, 암호화 단계의 처리에 의해 암호화된 콘텐츠, 및 키 정보 취득 단계의 처리에 의해 취득된 키 정보를, 파일 포맷으로 포맷화하고, 출력하는 포맷화 단계를 포함하는 것을 특징으로 한다.

본 발명의 제1 프로그램은, 콘텐츠를 취득하는 콘텐츠 취득 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는 워터마크를 추출하는 추출 단계와, 추출 단계의 처리에 의해 추출된 워터마크를 포함하는 헤더를 작성하는 헤더 작성 단계와, 비밀 키를 이용하여, 헤더 작성 단계의 처리에 의해 작성된 헤더의 데이터에 기초한 디지털 서명을 작성하는 디지털 서명 작성 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠를 암호화하는 암호화 단계와, 암호화 단계의 처리에 의해 암호화된 콘텐츠를 복호하는 데 필요한 키 정보를 포함하는 키 정보를 취득하는 키 정보 취득 단계와, 헤더 작성 단계의 처리에 의해 작성된 헤더, 디지털 서명 작성 단계의 처리에 의해 작성된 디지털 서명, 암호화 단계의 처리에 의해 암호화된 콘텐츠, 및 키 정보 취득 단계의 처리에 의해 취득된 키 정보를, 파일 포맷으로 포맷화하고, 출력하는 포맷화 단계를 컴퓨터에 실현시킨다.

본 발명의 제2 정보 처리 장치는, 암호화되어 있는 콘텐츠를 취득하는 콘텐츠 취득 수단과, 콘텐츠 취득 수단에 의해 취득된 콘텐츠에 부가되어 있는, 콘텐츠를 복호하는 데 필요한 키 정보를 검출하는 키 정보 검출 수단과, 키 정보 검출 수단에 의해 검출된 키 정보를 이용하여, 콘텐츠를 복호하는 데 필요한 콘텐츠 키를 취득하는 콘텐츠 키 취득 수단과, 콘텐츠 키 취득 수단에 의해 취득된 콘텐츠 키를 이용하여, 콘텐츠 취득 수단에 의해 취득된 콘텐츠를 복호하는 복호 수단과, 콘텐츠 취득 수단에 의해 취득된 콘텐츠에 부가되어 있는 증명서를 검출하는 증명서 검출 수단과, 증명서 검출 수단에 의해 검출된 증명서를, 인증국의 공개 키를 이용하여 검증하는 제1 검증 수단과, 증명서 검출 수단에 의해 검출된 증명서로부터, 콘텐츠를 제공하는 콘텐츠 제공자의 공개 키를 취득하는 공개 키 취득 수단과, 콘텐츠 취득 수단에 의해 취득된 콘텐츠에 부가되어 있는 디지털 서명을 검출하는 디지털 서명 검출 수단과, 디지털 서명 검출 수단에 의해 검출된 디지털 서명을, 공개 키 취득 수단에 의해 취득된 콘텐츠 제공자의 공개 키를 이용하여 검증하는 제2 검증 수단과, 콘텐츠 취득 수단에 의해 취득된 콘텐츠에 부가되어 있는 헤더로부터, 워터마크를 검출하는 워터마크 검출 수단과, 워터마

크 검출 수단에 의해 검출된 워터마크에 기초하여, 콘텐츠의 출력을 제어하는 제어 수단을 포함하는 것을 특징으로 한다.

본 발명의 제2 정보 처리 방법은, 암호화되어 있는 콘텐츠를 취득하는 콘텐츠 취득 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는, 콘텐츠를 복호하는 데 필요한 키 정보를 검출하는 키 정보 검출 단계와, 키 정보 검출 단계의 처리에 의해 검출된 키 정보를 이용하여, 콘텐츠를 복호하는 데 필요한 콘텐츠 키를 취득하는 콘텐츠 키 취득 단계와, 콘텐츠 키 취득 단계의 처리에 의해 취득된 콘텐츠 키를 이용하여, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠를 복호하는 복호 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는 증명서를 검출하는 증명서 검출 단계와, 증명서 검출 단계의 처리에 의해 검출된 증명서를, 인증국의 공개 키를 이용하여 검증하는 제1 검증 단계와, 증명서 검출 단계의 처리에 의해 검출된 증명서로부터, 콘텐츠 제공자의 공개 키를 취득하는 공개 키 취득 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는 디지털 서명을 검출하는 디지털 서명 검출 단계와, 디지털 서명 검출 단계의 처리에 의해 검출된 디지털 서명을, 공개 키 취득 단계의 처리에 의해 취득된 콘텐츠 제공자의 공개 키를 이용하여 검증하는 제2 검증 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는 헤더로부터, 워터마크를 검출하는 워터마크 검출 단계와, 워터마크 검출 단계의 처리에 의해 검출된 워터마크에 기초하여, 콘텐츠의 출력을 제어하는 제어 단계를 포함하는 것을 특징으로 한다.

본 발명의 제2 기록 매체의 프로그램은, 암호화되어 있는 콘텐츠를 취득하는 콘텐츠 취득 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는, 콘텐츠를 복호하는 데 필요한 키 정보를 검출하는 키 정보 검출 단계와, 키 정보 검출 단계의 처리에 의해 검출된 키 정보를 이용하여, 콘텐츠를 복호하는 데 필요한 콘텐츠 키를 취득하는 콘텐츠 키 취득 단계와, 콘텐츠 키 취득 단계의 처리에 의해 취득된 콘텐츠 키를 이용하여, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠를 복호하는 복호 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는 증명서를 검출하는 증명서 검출 단계와, 증명서 검출 단계의 처리에 의해 검출된 증명서를, 인증국의 공개 키를 이용하여 검증하는 제1 검증 단계와, 증명서 검출 단계의 처리에 의해 검출된 증명서로부터, 콘텐츠 제공자의 공개 키를 취득하는 공개 키 취득 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는 디지털 서명을 검출하는 디지털 서명 검출 단계와, 디지털 서명 검출 단계의 처리에 의해 검출된 디지털 서명을, 공개 키 취득 단계의 처리에 의해 취득된 콘텐츠 제공자의 공개 키를 이용하여 검증하는 제2 검증 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는 헤더로부터, 워터마크를 검출하는 워터마크 검출 단계와, 워터마크 검출 단계의 처리에 의해 검출된 워터마크에 기초하여, 콘텐츠의 출력을 제어하는 제어 단계를 포함하는 것을 특징으로 한다.

본 발명의 제2 프로그램은, 암호화되어 있는 콘텐츠를 취득하는 콘텐츠 취득 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는, 콘텐츠를 복호하는 데 필요한 키 정보를 검출하는 키 정보 검출 단계와, 키 정보 검출 단계의 처리에 의해 검출된 키 정보를 이용하여, 콘텐츠를 복호하는 데 필요한 콘텐츠 키를 취득하는 콘텐츠 키 취득 단계와, 콘텐츠 키 취득 단계의 처리에 의해 취득된 콘텐츠 키를 이용하여, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠를 복호하는 복호 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는 증명서를 검출하는 증명서 검출 단계와, 증명서 검출 단계의 처리에 의해 검출된 증명서를, 인증국의 공개 키를 이용하여 검증하는 제1 검증 단계와, 증명서 검출 단계의 처리에 의해 검출된 증명서로부터, 콘텐츠 제공자의 공개 키를 취득하는 공개 키 취득 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는 디지털 서명을 검출하는 디지털 서명 검출 단계와, 디지털 서명 검출 단계의 처리에 의해 검출된 디지털 서명을, 공개 키 취득 단계의 처리에 의해 취득된 콘텐츠 제공자의 공개 키를 이용하여 검증하는 제2 검증 단계와, 콘텐츠 취득 단계의 처리에 의해 취득된 콘텐츠에 부가되어 있는 헤더로부터, 워터마크를 검출하는 워터마크 검출 단계와, 워터마크 검출 단계의 처리에 의해 검출된 워터마크에 기초하여, 콘텐츠의 출력을 제어하는 제어 단계를 컴퓨터에 실현시킨다.

본 발명의 제1 정보 처리 장치 및 방법, 기록 매체, 및 프로그램에서는, 취득된 콘텐츠에 부가되어 있는 워터마크를 포함하는 헤더가 작성되고, 비밀 키를 이용하여, 그 작성된 헤더의 데이터에 기초한 디지털 서명이 작성되며, 취득된, 암호화된 콘텐츠를 복호하는 데 필요한 키 정보를 포함하는 키 정보가 취득되며, 헤더, 디지털 서명, 콘텐츠, 및 키 정보가, 파일 포맷으로 포맷화되어, 출력된다.

본 발명의 제2 정보 처리 장치 및 방법, 기록 매체, 및 프로그램에서는, 암호화되어 있는 콘텐츠를 복호하는 데 필요한 키 정보를 이용하여 취득된, 콘텐츠를 복호하는 데 필요한 콘텐츠 키를 이용하여 콘텐츠가 복호되고, 콘텐츠에 부가되어 있는 디지털 서명이, 콘텐츠를 제공하는 콘텐츠 제공자의 공개 키를 이용하여 검증되고, 콘텐츠에 부가되어 있는 헤더로부터 검출된 워터마크에 기초하여, 콘텐츠의 출력이 제어된다.

도면의 간단한 설명

도 1은 본 발명을 적용한 콘텐츠 제공 시스템의 구성을 도시한 블록도.

도 2는 도 1의 클라이언트의 구성을 도시한 블록도.

도 3은 도 1의 클라이언트의 콘텐츠의 다운로드 처리를 설명하는 흐름도.

도 4는 도 1의 콘텐츠 서버의 콘텐츠 제공 처리를 설명하는 흐름도.

도 5는 도 4의 단계 S26에서의 포맷 예를 도시한 도면.

도 6은 도 1의 클라이언트의 콘텐츠 재생 처리를 설명하는 흐름도.

도 7은 도 6의 단계 S43의 라이센스 취득 처리의 상세를 설명하는 흐름도.

도 8은 라이센스의 구성을 도시한 도면.

도 9는 도 1의 라이센스 서버의 라이센스 제공의 처리를 설명하는 흐름도.

도 10은 도 6의 단계 S45에서의 라이센스 갱신 처리의 상세를 설명하는 흐름도.

도 11은 도 1의 라이센스 서버의 라이센스 갱신 처리를 설명하는 흐름도.

도 12는 키의 구성을 설명하는 도면.

도 13은 카테고리 노드를 설명하는 도면.

도 14는 노드와 디바이스 대응의 구체예를 도시한 도면.

도 15A는 유효화 키 블록의 구성을 설명하는 도면.

도 15B는 유효화 키 블록의 구성을 설명하는 도면.

도 16은 유효화 키 블록의 이용을 설명하는 도면.

도 17은 유효화 키 블록의 포맷의 예를 도시한 도면.

도 18은 유효화 키 블록의 태그의 구성을 설명하는 도면.

도 19는 DNK를 이용한 콘텐츠의 복호 처리를 설명하는 도면.

도 20은 유효화 키 블록의 예를 도시한 도면.

도 21은 복수 콘텐츠의 하나의 디바이스에 대한 할당을 설명하는 도면.

도 22는 라이센스의 카테고리를 설명하는 도면.

도 23은 등록 처리를 설명하는 타이밍차트.

도 24는 클라이언트의 립핑 처리를 설명하는 흐름도.

도 25는 워터마크의 구성을 설명하는 도면.

도 26은 콘텐츠의 포맷 예를 도시한 도면.

도 27은 공개 키 증명서의 예를 도시한 도면.

도 28은 콘텐츠의 배포를 설명하는 도면.

도 29는 클라이언트의 콘텐츠의 체크아웃 처리를 설명하는 흐름도.

도 30은 태그에 의한 유효화 키 블록을 찾아가는 예를 설명하는 도면.

도 31은 유효화 키 블록의 구성예를 도시한 도면.

도 32는 마크의 구성을 설명하는 도면.

도 33은 클라이언트의 라이센스 매입 처리를 설명하는 흐름도.

도 34는 라이센스 서버의 라이센스 매입 처리를 설명하는 흐름도.

도 35는 마크의 구성예를 도시한 도면.

도 36은 클라이언트의 증명서의 등록 처리를 설명하는 흐름도.

도 37은 콘텐츠 서버의 증명서 등록 처리를 설명하는 흐름도.

도 38은 그룹 증명서의 예를 도시한 도면.

도 39는 그룹화가 행해지고 있는 경우에서의 콘텐츠 서버의 처리를 설명하는 흐름도.

도 40은 콘텐츠 키의 암호화의 예를 도시한 도면.

도 41은 그룹에 속하는 클라이언트의 처리를 설명하는 흐름도.

도 42는 다른 클라이언트에 라이센스를 체크아웃하는 클라이언트의 처리를 설명하는 흐름도.

도 43은 다른 클라이언트로부터 라이센스의 체크아웃을 받는 클라이언트의 처리를 설명하는 흐름도.

도 44는 라이센스의 체크아웃을 받은 클라이언트의 재생 처리를 설명하는 흐름도.

도 45는 다른 클라이언트로부터 라이센스의 체크인을 받는 클라이언트의 처리를 설명하는 흐름도.

도 46은 다른 클라이언트에 라이센스를 체크인하는 클라이언트의 처리를 설명하는 흐름도.

도 47은 MAC의 생성을 설명하는 도면.

도 48은 ICV 생성 키의 복호 처리를 설명하는 흐름도.

도 49는 ICV 생성 키의 다른 복호 처리를 설명하는 도면.

도 50A는 ICV에 의한 라이센스 복사의 관리를 설명하는 도면.

도 50B는 ICV에 의한 라이센스 복사의 관리를 설명하는 도면.

도 51은 라이센스의 관리를 설명하는 도면.

실시예

도 1은 본 발명을 적용한 콘텐츠 제공 시스템의 구성을 도시하고 있다. 인터넷(2)에는 클라이언트(1-1, 1-2)(이하, 이들 클라이언트를 개개로 구별할 필요가 없는 경우, 간단히 클라이언트(1)라 함)가 접속되어 있다. 이 예에서는 클라이언트가 2대만 도시되어 있지만, 인터넷(2)에는 임의의 수의 클라이언트가 접속된다.

또한, 인터넷(2)에는 클라이언트(1)에 대하여 콘텐츠를 제공하는 콘텐츠 서버(3), 콘텐츠 서버(3)가 제공하는 콘텐츠를 이용하는 데 필요한 라이센스를 클라이언트(1)에 대하여 부여하는 라이센스 서버(4), 및 클라이언트(1)가 라이센스를 수취한 경우에, 그 클라이언트(1)에 대하여 과금 처리를 행하는 과금 서버(5)가 접속되어 있다.

이들 콘텐츠 서버(3), 라이센스 서버(4) 및 과금 서버(5)도 임의의 수로 인터넷(2)에 접속된다.

도 2는 클라이언트(1)의 구성을 도시하고 있다.

도 2에 있어서, CPU(Central Processing Unit)(21)는 ROM(Read Only Memory)(22)에 기억되어 있는 프로그램, 또는 기억부(28)로부터 RAM(Random Access Memory)(23)에 로드된 프로그램에 따라서 각종 처리를 실행한다. 타이머(20)는 계시 동작을 행하고, 시각 정보를 CPU(21)에 공급한다. RAM(23)에는 또한 CPU(21)가 각종 처리를 실행하는 데에 필요한 데이터 등도 적절하게 기억된다.

암호화 복호부(24)는 콘텐츠 데이터를 암호화함과 함께, 이미 암호화되어 있는 콘텐츠 데이터를 복호하는 처리를 행한다. 코덱부(25)는 예를 들면, ATRAC(Adaptive Transform Acoustic Coding)3 방식 등으로 콘텐츠 데이터를 인코딩하고, 입출력 인터페이스(32)를 통해 드라이브(30)에 접속되어 있는 반도체 메모리(44)에 공급하여 기록시킨다. 및/또는, 코덱부(25)는 드라이브(30)를 통해 반도체 메모리(44)로부터 판독한, 인코딩되어 있는 데이터를 디코딩한다.

반도체 메모리(44)는 예를 들면, 메모리스틱(상표) 등으로 구성된다.

CPU(21), ROM(22), RAM(23), 암호화 복호부(24) 및 코덱부(25)는 버스(31)를 통해 서로 접속되어 있다. 이 버스(31)에는 또한 입출력 인터페이스(32)도 접속되어 있다.

입출력 인터페이스(32)에는 키보드와 마우스 등으로 이루어지는 입력부(26), CRT와 LCD 등으로 이루어지는 디스플레이, 및 스피커 등으로 이루어지는 출력부(27), 하드디스크 등으로 구성되는 기억부(28), 모뎀, 터미널 어댑터 등으로 구성되는 통신부(29)가 접속되어 있다. 통신부(29)는 인터넷(2)을 통한 통신 처리를 행한다. 통신부(29)는 또한, 다른 클라이언트와의 사이에서 아날로그 신호 또는 디지털 신호의 통신 처리를 행한다.

입출력 인터페이스(32)에는 또한, 필요에 따라서 드라이브(30)가 접속되고, 자기 디스크(41), 광 디스크(42), 광 자기 디스크(43), 혹은 반도체 메모리(44) 등이 적절하게 장착되고, 이들로부터 판독된 컴퓨터 프로그램이 필요에 따라서 기억부(28)에 인스톨된다.

또한, 도시는 생략하지만, 콘텐츠 서버(3), 라이센스 서버(4), 과금 서버(5)도, 도 2에 도시한 클라이언트(1)와 기본적으로 마찬가지 구성을 갖는 컴퓨터로 구성된다. 따라서, 이하의 설명에서는, 도 2의 구성은 콘텐츠 서버(3), 라이센스 서버(4), 과금 서버(5) 등의 구성으로서도 인용된다.

다음에, 도 3의 흐름도를 참조하여, 클라이언트(1)가 콘텐츠 서버(3)로부터 콘텐츠의 제공을 받는 처리에 대하여 설명한다.

사용자가 입력부(26)를 조작함으로써 콘텐츠 서버(3)에 대한 액세스를 지령하면, CPU(21)은 단계 S1에 있어서, 통신부(29)를 제어하고, 인터넷(2)을 통해 콘텐츠 서버(3)를 액세스시킨다. 단계 S2에 있어서, 사용자가 입력부(26)를 조작하여 제공 받을 콘텐츠를 지정하면, CPU(21)는 이 지정 정보를 수취하고, 통신부(29)로부터, 인터넷(2)을 통해 콘텐츠 서버(3)에, 지정된 콘텐츠를 통지한다. 도 4의 흐름도를 참조하여 후술하는 바와 같이, 이 통지를 받은 콘텐츠 서버(3)는 암호화된 콘텐츠 데이터를 송신하여 오기 때문에, 단계 S3에 있어서, CPU(21)는 통신부(29)를 통해 이 콘텐츠 데이터를 수신하면, 단계 S4에 있어서, 그 암호화되어 있는 콘텐츠 데이터를 기억부(28)를 구성하는 하드디스크에 공급하여 기억시킨다.

다음에, 도 4의 흐름도를 참조하여, 클라이언트(1)의 이상의 처리에 대응하는 콘텐츠 서버(3)의 콘텐츠 제공 처리에 대하여 설명한다. 또, 이하의 설명에 있어서, 도 2의 클라이언트(1)의 구성은 콘텐츠 서버(3)의 구성으로서도 인용된다.

단계 S21에 있어서, 콘텐츠 서버(3)의 CPU(21)는, 인터넷(2)으로 통신부(29)를 통해 클라이언트(1)로부터 액세스를 받을 때까지 대기하다가, 액세스를 받았다고 판정하였을 때, 단계 S22로 진행하여, 클라이언트(1)로부터 송신되어 온 콘텐츠를 지정하는 정보를 저장한다. 이 콘텐츠를 지정하는 정보는 클라이언트(1)가 도 3의 단계 S2에서 통지되어 온 정보이다.

단계 S23에 있어서, 콘텐츠 서버(3)의 CPU(21)는, 기억부(28)에 기억되어 있는 콘텐츠 데이터 중에서, 단계 S22의 처리에서 취득된 정보에 의해 지정된 콘텐츠를 판독한다. CPU(21)는 단계 S24에 있어서, 기억부(28)로부터 판독된 콘텐츠 데이터를 암호화 복호부(24)에 공급하고, 콘텐츠 키 Kc를 이용하여 암호화시킨다.

기억부(28)에 기억되어 있는 콘텐츠 데이터는 코덱부(25)에 의해 이미 ATRAC3 방식에 의해 인코딩되어 있기 때문에, 이 인코딩되어 있는 콘텐츠 데이터가 암호화되게 된다.

또한 물론, 기억부(28)에 미리 암호화한 상태로 콘텐츠 데이터를 기억시킬 수 있다. 이 경우에는 단계 S24의 처리는 생략하는 것이 가능하다.

다음에, 단계 S25에 있어서, 콘텐츠 서버(3)의 CPU(21)는 암호화한 콘텐츠 데이터를 전송하는 포맷을 구성하는 헤더에, 암호화되어 있는 콘텐츠를 복호하는 데 필요한 키 정보(도 5를 참조하여 후술하는 EKB(Enabling Key Block)와 K_{EKBC} (Kc))와, 콘텐츠를 이용하는 데 필요한 라이센스를 식별하기 위한 라이센스 ID를 부가한다. 그리고, 단계 S26에 있어서, 콘텐츠 서버(3)의 CPU(21)는, 단계 S24의 처리에서 암호화한 콘텐츠와, 단계 S25의 처리에서 키와 라이센스 ID를 부가한 헤더를 포맷화한 데이터를 통신부(29)로부터 인터넷(2)을 통해 액세스해 온 클라이언트(1)에 송신한다.

도 5는 이와 같이 하여, 콘텐츠 서버(3)로부터 클라이언트(1)에 콘텐츠가 공급되는 경우의 포맷의 구성을 도시하고 있다. 도 5에 도시한 바와 같이, 이 포맷은 헤더(Header)와 데이터(Data)로 구성된다.

헤더에는 콘텐츠 정보(Content Information), URL(Uniform Resource Locator), 라이센스 ID(License ID), 인에이블링 키 블록(유효화 키 블록)(EKB(Enabling Key Block)) 및, EKB에서 생성된 키 K_{EKBC} 를 이용하여 암호화된 콘텐츠 키 Kc로서의 데이터 K_{EKBC} (Kc)가 배치되어 있다. 또, EKB에 대해서는 도 15 A 및 도 15B를 참조하여 후술한다.

콘텐츠 정보에는 데이터로서 포맷화되어 있는 콘텐츠 데이터를 식별하기 위한 식별 정보로서의 콘텐츠 ID(CID), 그 콘텐츠의 코덱 방식 등의 정보가 포함되어 있다.

URL은 라이센스 ID로 규정되는 라이센스를 취득할 때 액세스하는 어드레스 정보이며, 도 1의 시스템의 경우, 구체적으로는 라이센스를 받기 위해서 필요한 라이센스 서버(4)의 어드레스이다. 라이센스 ID는 데이터로서 기록되어 있는 콘텐츠를 이용할 때 필요로 하는 라이센스를 식별하는 것이다.

데이터는 임의의 수의 암호화 블록(Encryption Block)으로 구성된다. 각 암호화 블록은 이니셜 벡터(IV(Initial Vector)), 시드(Seed), 및 콘텐츠 데이터를 키 K'c로 암호화한 데이터 EK'c(data)로 구성되어 있다.

키 K'c는 다음 식에 의해 나타내진 바와 같이, 콘텐츠 키 Kc와, 난수로 설정되는 값 Seed를 해시 함수에 적용하여 연산된 값으로 구성된다.

K'c=Hash(Kc, Seed)

이니셜 벡터 IV와 시드 Seed는 각 암호화 블록마다 서로 다른 값으로 설정된다.

이 암호화는 콘텐츠의 데이터를 8 바이트 단위로 구분하고, 8 바이트마다 행해진다. 후단의 8 바이트의 암호화는 전단의 8 바이트의 암호화 결과를 이용하여 행해지는 CBC(Cipher Block Chaining) 모드로 행해진다.

CBC 모드의 경우, 최초의 8 바이트의 콘텐츠 데이터를 암호화할 때, 그 전단의 8 바이트의 암호화 결과가 존재하지 않기 때문에, 최초의 8 바이트의 콘텐츠 데이터를 암호화할 때는, 이니셜 벡터 IV를 초기값으로 하여 암호화가 행해진다.

이 CBC 모드에 의한 암호화를 행함으로써, 하나의 암호화 블록이 해독되었다고 하여도, 그 영향이 다른 암호화 블록에 미치는 것이 억제된다.

또, 이 암호화에 대하여는 도 47을 참조하여 후에 상술한다.

또한, 암호 방식에 대해서는 이것에 한하지 않고, 단순히 콘텐츠 키 Kc로 콘텐츠 데이터를 암호화하여도 된다.

이상과 같이 하여, 클라이언트(1)는 콘텐츠 서버(3)로부터 콘텐츠를 무료로 자유롭게 취득할 수 있다. 따라서, 콘텐츠 그 자체는 대량으로 배포하는 것이 가능해진다.

그러나, 각 클라이언트(1)는 취득한 콘텐츠를 이용할 때, 라이센스를 유지하고 있을 필요가 있다. 따라서, 도 6을 참조하여, 클라이언트(1)가 콘텐츠를 재생하는 경우의 처리에 대하여 설명한다.

단계 S41에 있어서, 클라이언트(1)의 CPU(21)는 사용자가 입력부(26)를 조작함으로써 지시한 콘텐츠의 식별 정보(CID)를 취득한다. 이 식별 정보는 예를 들면, 콘텐츠의 타이틀이나, 기억되어 있는 각 콘텐츠마다 부여되어 있는 번호 등으로 구성된다.

그리고, CPU(21)는, 콘텐츠가 지시되면, 그 콘텐츠에 대응하는 라이센스 ID(그 콘텐츠를 사용하는 데 필요한 라이센스의 ID)를 판독한다. 이 라이센스 ID는 도 5에 도시한 바와 같이, 암호화되어 있는 콘텐츠 데이터의 헤더에 기술되어 있는 것이다.

다음에, 단계 S42로 진행하여, CPU(21)는, 단계 S41에서 판독된 라이센스 ID에 대응하는 라이센스가, 클라이언트(1)에 의해 이미 취득되고, 기억부(28)에 기억되어 있는지의 여부를 판정한다. 아직 라이센스가 취득되어 있지 않은 경우에는, 단계 S43으로 진행하여, CPU(21)는 라이센스 취득 처리를 실행한다. 이 라이센스 취득 처리의 상세는 도 7의 흐름도를 참조하여 후술한다.

단계 S42에 있어서, 라이센스가 이미 취득되어 있다고 판정된 경우, 또는 단계 S43에 있어서, 라이센스 취득 처리가 실행된 결과, 라이센스가 취득된 경우, 단계 S44로 진행하고, CPU(21)는 취득되어 있는 라이센스가 유효 기한 내의 것인지의 여부를 판정한다. 라이센스가 유효 기한 내의 것인지의 여부는, 라이센스의 내용으로서 규정되어 있는 기한(후술하는 도 8 참조)과, 타이머(20)에 의해 계시되는 현재 일시를 비교함으로써 판단된다. 라이센스의 유효 기한이 이미 만료되었다고 판정된 경우, CPU(21)는 단계 S45로 진행하여, 라이센스 갱신 처리를 실행한다. 이 라이센스 갱신 처리의 상세는 도 10의 흐름도를 참조하여 후술한다.

단계 S44에 있어서, 라이센스는 아직 유효 기한 내라고 판정된 경우, 또는, 단계 S45에 있어서, 라이센스가 갱신된 경우, 단계 S46으로 진행하고, CPU(21)는 암호화되어 있는 콘텐츠 데이터를 기억부(28)로부터 판독하여 RAM(23)에 저장시킨다. 그리고, 단계 S47에서 CPU(21)는, RAM(23)에 기억된 암호화 블록의 데이터를, 도 5의 데이터에 배치되어 있는 암호화 블록 단위로 암호화 복호부(24)에 공급하고, 콘텐츠 키 Kc를 이용하여 복호시킨다.

콘텐츠 키 Kc를 얻는 방법의 구체예는 도 15A 및 도 15B를 참조하여 후술하지만, 디바이스 노드 키(DNK(Device Node Key))를 이용하여, EKB(도 5)에 포함되는 키 K_{EKBC} 를 얻을 수 있고, 그 키 K_{EKBC} 를 이용하여, 데이터 K_{EKBC} (Kc)(도 5)로부터 콘텐츠 키 Kc를 얻을 수 있다.

CPU(21)는 또한, 단계 S48에 있어서, 암호화 복호부(24)에 의해 복호된 콘텐츠 데이터를 코덱부(25)에 공급하여 디코딩시킨다. 그리고, 코덱부(25)에 의해 디코딩된 데이터를, CPU(21)는 입출력 인터페이스(32)로부터 출력부(27)에 공급하고 D/A 변환시켜, 스피커로부터 출력시킨다.

다음에, 도 7의 흐름도를 참조하여, 도 6의 단계 S43에서 행해지는 라이센스 취득 처리의 상세에 대하여 설명한다.

클라이언트(1)는 사전에 라이센스 서버를 액세스하여 등록 처리를 행함으로써, 리프 ID, DNK(Device Node Key), 클라이언트(1)의 비밀 키· 공개 키의 쌍, 라이센스 서버의 공개 키, 및 각 공개 키의 증명서를 포함하는 서비스 데이터를 취득해 둔다. 클라이언트의 등록 처리의 상세는 도 23을 참조하여 후술한다.

리프 ID는 클라이언트마다 할당된 식별 정보를 나타내고, DNK는 그 라이센스에 대응하는 EKB(유효화 키 블록)에 포함되는 암호화되어 있는 콘텐츠 키 Kc를 복호하는 데 필요한 디바이스 노드 키이다(도 12를 참조하여 후술함).

처음에 단계 S61에 있어서, CPU(21)는, 지금 처리 대상으로 되어 있는 라이센스 ID에 대응하는 URL을 도 5에 도시한 헤더로부터 취득한다. 상술한 바와 같이, 이 URL은 역시 헤더에 기술되어 있는 라이센스 ID에 대응하는 라이센스를 취득할 때 액세스하여야 할 어드레스이다. 따라서, 단계 S62에 있어서, CPU(21)는 단계 S61에서 취득한 URL에 액세스한다. 구체적으로는, 통신부(29)에 의해 인터넷(2)을 통해 라이센스 서버(4)에 액세스가 행해진다. 이 때, 라이센스 서버(4)는 클라이언트(1)에 대하여, 구입할 라이센스(콘텐츠를 사용하는 데에 필요한 라이센스)를 지정하는 라이센스 지정 정보, 및 사용자 ID와 패스워드의 입력을 요구한다(후술하는 도 9의 단계 S102). CPU(21)는 이 요구를 출력부(27)의 표시부에 표시시킨다. 사용자는 이 표시에 기초하여 입력부(26)를 조작하여, 라이센스 지정 정보, 사용자 ID, 및 패스워드를 입력한다. 또, 이 사용자 ID와 패스워드는 클라이언트(1)의 사용자가 인터넷(2)을 통해 라이센스 서버(4)에 액세스하여 사전에 취득해 둔 것이다.

CPU(21)는 단계 S63, S64에 있어서, 입력부(26)로부터 입력된 라이센스 지정 정보를 저장함과 함께, 사용자 ID와 패스워드를 저장한다. CPU(21)는 단계 S65에 있어서, 통신부(29)를 제어하여, 입력된 사용자 ID와 패스워드, 라이센스 지정 정보, 및 서비스 데이터(후술함)에 포함되는 리프 ID를 포함하는 라이센스 요구를, 인터넷(2)을 통해 라이센스 서버(4)에 송신시킨다.

라이센스 서버(4)는 도 9를 참조하여 후술하는 바와 같이, 사용자 ID와 패스워드 및 라이센스 지정 정보에 기초하여 라이센스를 송신(단계 S109)한다든가, 또는, 조건이 만족되지 않은 경우에는, 라이센스를 송신하지 않는다(단계 S112).

단계 S66에 있어서, CPU(21)는 라이센스 서버(4)로부터 라이센스가 송신되었는지의 여부를 판정하고, 라이센스가 송신되어 온 경우에는, 단계 S67로 진행하여, 그 라이센스를 기억부(28)에 공급하여 기억시킨다.

단계 S66에 있어서, 라이센스가 송신되어 오지 않는다고 판정한 경우, CPU(21)는 단계 S68로 진행하여, 에러 처리를 실행한다. 구체적으로는, CPU(21)는 콘텐츠를 이용하기 위한 라이센스가 얻어지지 않으므로, 콘텐츠의 재생 처리를 금지한다.

이상과 같이 하여, 각 클라이언트(1)는 콘텐츠 데이터에 부수하고 있는 라이센스 ID에 대응하는 라이센스를 취득하여, 비로소 그 콘텐츠를 사용하는 것이 가능해진다.

또, 도 7의 라이센스 취득 처리는 각 사용자가 콘텐츠를 취득하기 전에 미리 행하여 두도록 하는 것도 가능하다.

클라이언트(1)에 제공되는 라이센스는, 예를 들면 도 8에 도시한 바와 같이 사용 조건, 리프 ID 등을 포함하고 있다.

사용 조건에는 그 라이센스에 기초하여 콘텐츠를 사용하는 것이 가능한 사용 기한, 그 라이센스에 기초하여 콘텐츠를 다운로드하는 것이 가능한 다운로드 기한, 그 라이센스에 기초하여 콘텐츠를 복사하는 것이 가능한 횟수(허용되는 복사 횟수), 체크아웃 횟수, 최대 체크아웃 횟수, 그 라이센스에 기초하여, 콘텐츠를 CD-R에 기록할 수 있는 권리, PD(Portable Device)에 복사하는 것이 가능한 횟수, 라이센스를 소유권(매입 상태)으로 이행할 수 있는 권리, 사용 로그를 취할 의무 등을 나타내는 정보가 포함된다.

다음에, 도 9의 흐름도를 참조하여, 도 7의 클라이언트(1)의 라이센스 취득 처리에 대응하여 실행되는 라이센스 서버(4)의 라이센스 제공 처리에 대하여 설명한다. 또, 이 경우에서도 도 2의 클라이언트(1)의 구성은 라이센스 서버(4)의 구성으로서 인용된다.

단계 S101에 있어서, 라이센스 서버(4)의 CPU(21)는 클라이언트(1)로부터 액세스를 받을 때까지 대기하고, 액세스를 받았을 때, 단계 S102로 진행하고, 액세스해 온 클라이언트(1)에 대하여 사용자 ID와 패스워드, 및 라이센스 지정 정보의 송신을 요구한다. 상술한 바와 같이 하여, 클라이언트(1)로부터, 도 7의 단계 S65의 처리에서, 사용자 ID와 패스워드, 리프 ID 및 라이센스 지정 정보(라이센스 ID)가 송신되어 왔을 때, 라이센스 서버(4)의 CPU(21)는, 통신부(29)를 통해 이것을 수신하고, 저장하는 처리를 실행한다.

그리고, 라이센스 서버(4)의 CPU(21)는, 단계 S103에 있어서, 통신부(29)로부터 과금 서버(5)에 액세스하여, 사용자 ID와 패스워드에 대응하는 사용자의 여신 처리를 요구한다. 과금 서버(5)는 인터넷(2)을 통해 라이센스 서버(4)로부터 여신 처리의 요구를 받으면, 그 사용자 ID와 패스워드에 대응하는 사용자의 과거의 지불 이력 등을 조사하고, 그 사용자가, 과거에 라이센스 대가의 미불 실적이 있는지의 여부 등을 조사하여, 그와 같은 실적이 없는 경우에는, 라이센스의 부여를 허용하는 여신 결과를 송신하고, 미불 실적 등이 있는 경우에는, 라이센스 부여 불허가의 여신 결과를 송신한다.

단계 S104에 있어서, 라이센스 서버(4)의 CPU(21)는, 과금 서버(5)로부터의 여신 결과가 라이센스를 부여하는 것을 허용하는 여신 결과인지의 여부를 판정하고, 라이센스의 부여가 허용되어 있는 경우에는, 단계 S105로 진행하여, 단계 S102의 처리에서 취득된 라이센스 지정 정보에 대응하는 라이센스를, 기억부(28)에 기억되어 있는 라이센스 중에서 추출한다. 기억부(28)에 기억되어 있는 라이센스는, 미리 라이센스 ID, 버전, 작성 일시, 유효 기한 등의 정보가 기술되어 있다. 단계 S106에 있어서, CPU(21)는 그 라이센스에 수신한 리프 ID를 부가한다. 또한, 단계 S107에 있어서, CPU(21)는 단계 S105에서 선택된 라이센스에 대응지워져 있는 사용 조건을 선택한다. 및/또는, 단계 S102의 처리에서, 사용자로부터 사용 조건이 지정된 경우에는, 그 사용 조건이 필요에 따라서, 미리 준비되어 있는 사용 조건에 부가된다. CPU(21)는 선택된 사용 조건을 라이센스에 부가한다.

단계 S108에 있어서, CPU(21)는 라이센스 서버의 비밀 키에 의해 라이센스에 서명하고, 이에 의해, 도 8에 도시한 바와 같은 구성의 라이센스가 생성된다.

다음에, 단계 S109로 진행하여, 라이센스 서버(4)의 CPU(21)는 그 라이센스(도 8에 도시한 구성을 갖음)를 통신부(29)로부터 인터넷(2)을 통해 클라이언트(1)에 송신시킨다.

단계 S110에 있어서 라이센스 서버(4)의 CPU(21)는, 단계 S109의 처리에서, 지금 송신한 라이센스(사용 조건, 리프 ID를 포함함)를, 단계 S102의 처리에서 취득된 사용자 ID와 패스워드에 대응하여 기억부(28)에 기억시킨다. 또한, 단계 S111에 있어서, CPU(21)는 과금 처리를 실행한다. 구체적으로는, CPU(21)는 통신부(29)로부터 과금 서버(5)에, 그 사용자 ID와 패스워드에 대응하는 사용자에 대한 과금 처리를 요구한다. 과금 서버(5)는 이 과금의 요구에 기초하여 그 사용자에 대한 과금 처리를 실행한다. 상술한 바와 같이, 이 과금 처리에 대하여 그 사용자가 지불을 행하지 않은 경우에는, 이후, 그 사용자는 라이센스 부여를 요구하였다고 해도, 라이센스를 받을 수 없게 된다.

즉, 이 경우에는 과금 서버(5)로부터 라이센스 부여를 불허가로 하는 여신 결과가 송신되어 오기 때문에, 단계 S104에서 단계 S112로 진행하여, CPU(21)는 에러 처리를 실행한다. 구체적으로는, 라이센스 서버(4)의 CPU(21)는, 통신부(29)를 제어하여 액세스해 온 클라이언트(1)에 대하여, 라이센스를 부여할 수 없다는 취지의 메시지를 출력하고, 처리를 종료시킨다.

이 경우, 상술한 바와 같이, 그 클라이언트(1)는 라이센스를 받을 수 없기 때문에, 그 콘텐츠를 이용하는 것(암호를 복호하는 것)을 할 수 없게 된다.

도 10은 도 6의 단계 S45에서의 라이센스 갱신 처리의 상세를 도시하고 있다. 도 10의 단계 S131 내지 단계 S135의 처리는 도 7의 단계 S61 내지 단계 S65의 처리와 기본적으로 마찬가지 처리이다. 단, 단계 S133에 있어서, CPU(21)는 구입할 라이센스가 아니라, 갱신할 라이센스의 라이센스 ID를 저장한다. 그리고, 단계 S135에 있어서, CPU(21)는 사용자 ID와 패스워드와 함께, 갱신할 라이센스의 라이센스 ID를 라이센스 서버(4)에 송신한다.

단계 S135의 송신 처리에 대응하여, 라이센스 서버(4)는 후술하는 바와 같이 사용 조건을 제시해 온다(도 11의 단계 S153). 따라서, 클라이언트(1)의 CPU(21)는 단계 S136에 있어서, 라이센스 서버(4)로부터의 사용 조건 제시를 수신하고, 이것을 출력부(27)에 출력하여 표시시킨다. 사용자는 입력부(26)를 조작하고, 이 사용 조건 중에서 소정의 사용 조건을 선택하거나 소정의 사용 조건을 새롭게 추가하기도 한다. 단계 S137에서 CPU(21)는 이상과 같이 하여 선택된 사용 조건(라이센스를 갱신하는 조건)을 구입하기 위한 신청을 라이센스 서버(4)에 송신한다. 이 신청에 대응하여, 후술하는 바와 같이 라이센스 서버(4)는 최종적인 사용 조건을 송신해 온다(도 11의 단계 S154). 따라서, 단계 S138에 있어서, 클라이언트(1)의 CPU(21)는 라이센스 서버(4)로부터의 사용 조건을 취득하고, 단계 S139에 있어서, 그 사용 조건을 기억부(28)에 이미 기억되어 있는 대응하는 라이센스의 사용 조건으로서 갱신한다.

도 11은 이상의 클라이언트(1)의 라이센스 갱신 처리에 대응하여 라이센스 서버(4)가 실행하는 라이센스 갱신 처리를 도시하고 있다.

처음에, 단계 S151에 있어서, 라이센스 서버(4)의 CPU(21)는, 클라이언트(1)로부터의 액세스를 받으면, 단계 S152에 있어서, 클라이언트(1)가 단계 S135에서 송신한 라이센스 지정 정보를 라이센스 갱신 요구 정보와 함께 수신한다.

단계 S153에 있어서, CPU(21)는 라이센스의 갱신 요구를 수신하면, 그 라이센스에 대응하는 사용 조건(갱신하는 사용 조건)을 기억부(28)로부터 판독하여, 클라이언트(1)에 송신한다.

이 제시에 대하여, 상술한 바와 같이, 클라이언트(1)로부터 사용 조건의 구입이 도 10의 단계 S137의 처리에서 신청되면, 단계 S154에 있어서, 라이센스 서버(4)의 CPU(21)는 신청된 사용 조건에 대응하는 데이터를 생성하고, 단계 S154에 있어서, 클라이언트(1)에 송신한다. 클라이언트(1)는 상술한 바와 같이, 단계 S139의 처리에서 수신한 사용 조건을 이용하여, 이미 등록되어 있는 라이센스의 사용 조건을 갱신한다.

본 발명에서는 도 12에 도시한 바와 같이, 브로드캐스트 인크립션(Broadcast Encryption) 방식의 원리에 기초하여 디바이스와 라이센스의 키가 관리된다(일본 특허 공개2001-352321호 공보 참조). 키는 계층 트리 구조로 되고, 최하단의 리프(leaf)가 개개의 디바이스의 키에 대응한다. 도 12의 예의 경우, 번호 0에서 번호 15까지의 16개의 디바이스 또는 라이센스에 대응하는 키가 생성된다.

각 키는 도면 중 동그라미 표시로 나타내는 트리 구조의 각 노드에 대응하여 규정된다. 이 예에서는 최상단의 루트 노드에 대응하여 루트 키 KR이, 2단째의 노드에 대응하여 키 K0, K1이, 3단째의 노드에 대응하여 키 K00 내지 K11이, 제4단째의 노드에 대응하여 키 K000 내지 키 K111이, 각각 대응되어 있다. 그리고, 최하단의 노드로서의 리프(디바이스 노드)에, 키 K0000 내지 K1111이 각각 대응되어 있다.

계층 구조로 되어 있기 때문에, 예를 들면, 키 K0010과 키 0011의 상위의 키는 K001이 되고, 키 K000과 키 K001의 상위의 키는 K00으로 되어 있다. 이하 마찬가지로, 키 K00과 키 K01의 상위의 키는 K0이 되고, 키 K0과 키 K1의 상위의 키는 KR로 되어 있다.

콘텐츠를 이용하는 키는 최하단의 리프에서 최상단의 루트 노드까지의 하나의 패스의 각 노드에 대응하는 키로 관리된다. 예를 들면, 번호 3의 노드(리프 ID)에 대응하는 라이센스에 기초하여 콘텐츠를 이용하는 키는, 키 K0011, K001, K00, K0, KR을 포함하는 패스의 각 키에 의해 관리된다.

본 발명의 시스템에서는 도 13에 도시한 바와 같이, 도 12의 원리에 기초하여 구성되는 키 시스템으로, 디바이스 키와 라이센스 키의 관리가 행해진다. 도 13의 예에서는 8+24+32단의 노드가 트리 구조로 되고, 루트 노드에서 하위 8단까지의 각 노드에 카테고리가 대응된다. 여기에서의 카테고리란, 예를 들면 메모리스틱 등의 반도체 메모리를 사용하는 기기의 카테고리, 디지털 방송을 수신하는 기기의 카테고리라고 하는 카테고리를 의미한다. 그리고, 이 카테고리 노드 중 하나의 노드에, 라이센스를 관리하는 시스템으로서 본 시스템(T 시스템이라 함)이 대응한다.

즉, 이 T 시스템의 노드보다 더 아래 계층의 24단의 노드에 대응하는 키에 의해 라이센스가 대응된다. 이 예의 경우, 이것에 의해, 2의 24승(약 16메가)의 라이센스를 규정할 수 있다. 또한, 가장 하측의 32단의 계층에 의해, 2의 32승(약 4기가)의 사용자(혹은 클라이언트(1))를 규정할 수 있다. 최하단의 32단의 노드에 대응하는 리프에서 루트 노드까지의 패스의 각 노드에 대응하는 키가, DNK(Device Node Key)를 구성하고, 최하단의 리프에 대응하는 ID가 리프 ID로 된다.

각 디바이스나 라이센스의 키는 64(=8+24+32)단의 각 노드로 구성되는 패스의 내의 하나에 대응된다. 예를 들면, 콘텐츠를 암호화한 콘텐츠 키는, 대응하는 라이센스에 할당된 패스를 구성하는 노드에 대응하는 키를 이용하여 암호화된다. 상위 계층의 키는 그 바로 근처의 하위 계층의 키를 이용하여 암호화되고, EKB(도 15A 및 도 15B를 참조하여 후술함) 내에 배치된다. DNK는 EKB 내에는 배치되지 않고, 서비스 데이터에 기술되고, 사용자의 클라이언트(1)에 주어진다. 클라이언트(1)는 서비스 데이터에 기술되어 있는 DNK를 이용하여, 콘텐츠 데이터와 함께 배포되는 EKB(도 15A 및 도 15B) 내에 기술되어 있는 바로 근처의 상위 계층의 키를 복호하고, 복호하여 얻은 키를 이용하여, EKB 내에 기술되어 있는 더 상위 계층의 키를 복호한다. 이상의 처리를 순차적으로 행함으로써, 클라이언트(1)는 그 패스에 속하는 모든 키를 얻을 수 있다.

도 14에 계층 트리 구조의 카테고리 분류의 구체적인 예를 도시한다. 도 14에 있어서, 계층 트리 구조의 최상단에는 루트 키 KR(2301)이 설정되고, 이하의 중간단에는 노드 키(2302)가 설정되고, 최하단에는 리프 키(2303)가 설정된다. 각 디바이스는 개개의 리프 키와, 리프 키로부터 루트 키에 이르는 일련의 노드 키, 루트 키를 보유한다.

최상단으로부터 제M 단째(도 13의 예에서는 M=8)의 소정 노드가 카테고리 노드(2304)로서 설정된다. 즉 제M 단째의 노드 각각이 특정 카테고리의 디바이스 설정 노드가 된다. 제M 단의 하나의 노드를 정점으로 하여 M+1단 이하의 노드 및 리프는, 그 카테고리에 포함되는 디바이스에 관한 노드 및 리프가 된다.

예를 들면 도 14의 제M 단째의 하나의 노드(2305)에는 카테고리 [메모리스틱(상표)]가 설정되고, 이 노드 이하에 연속해 있는 노드 및 리프는 메모리스틱을 사용한 여러 가지 디바이스를 포함하는 카테고리 전용의 노드 또는 리프로서 설정된다. 즉, 노드(2305) 이하가, 메모리스틱의 카테고리로 정의되는 디바이스의 관련 노드 및 리프의 집합으로서 정의된다.

또한, M단부터 수단분 하위의 단을 서브 카테고리 노드(2306)로서 설정할 수 있다. 도 14의 예에서는 카테고리 [메모리스틱] 노드(2305)의 2단 아래의 노드에, 메모리스틱을 사용한 디바이스의 카테고리에 포함되는 서브 카테고리 노드로서, [재생 전용기]의 노드(2306)가 설정되어 있다. 또한, 서브 카테고리 노드인 재생 전용기의 노드(2306) 이하에, 재생 전용기의 카테고리에 포함되는 음악 재생 기능을 갖는 전화의 노드(2307)가 설정되고, 또한 그 하위에, 음악 재생 기능을 갖는 전화의 카테고리에 포함되는 [PHS] 노드(2308)와, [휴대 전화] 노드(2309)가 설정되어 있다.

또한, 카테고리와 서브 카테고리는 디바이스의 종류뿐만 아니라, 예를 들면 어떤 메이커, 콘텐츠 프로바이더, 결제 기관 등이 독자적으로 관리하는 노드, 즉 처리 단위, 관할 단위, 혹은 제공 서비스 단위 등, 임의의 단위(이들을 총칭하여 이하, 엔티티라 함)로 설정하는 것이 가능하다. 예를 들면 하나의 카테고리 노드를 게임 기기 메이커가 판매하는 게임 기기 XYZ 전용의 정점 노드로서 설정하면, 메이커가 판매하는 게임 기기 XYZ에, 그 정점 노드 이하의 하단의 노드 키, 리프 키를 저장하고 판매하는 것이 가능해지고, 그 후, 암호화 콘텐츠의 배신, 혹은 각종 키의 배신 및 갱신 처리를, 그 정점 노드 키 이하의 노드 키, 리프 키에 의해서 구성되는 유효화 키 블록(EKB)을 생성하여 배신하고, 정점 노드 이하의 디바이스에 대해서만 이용 가능한 데이터가 배신 가능해진다.

이와 같이, 하나의 노드를 정점으로 하여, 이하의 노드를 그 정점 노드로 정의된 카테고리 혹은 서브 카테고리의 관련 노드로서 설정하는 구성으로 함으로써, 카테고리단 혹은 서브 카테고리단의 하나의 정점 노드를 관리하는 메이커, 콘텐츠 프로바이더 등이 그 노드를 정점으로 하는 유효화 키 블록(EKB)을 독자적으로 생성하고, 정점 노드 이하에 속하는 디바이스에 배신하는 구성이 가능해져, 정점 노드에 속하지 않는 다른 카테고리의 노드에 속하는 디바이스에는 전혀 영향을 미치게 하지 않고서 키 갱신을 실행할 수 있다.

예를 들면, 도 12에 도시한 트리 구조에 있어서, 하나의 그룹에 포함되는 4개의 디바이스 0, 1, 2, 3은 노드 키로서 공통의 키 K00, K0, KR을 보유한다. 이 노드 키 공유 구성을 이용함으로써, 공통의 콘텐츠 키를 디바이스 0, 1, 2, 3에만 제공하는 것이 가능해진다. 예를 들면, 공통으로 보유하는 노드 키 K00 자체를 콘텐츠 키로서 설정하면, 새로운 키 송부를 실행하지 않고 디바이스 0, 1, 2, 3만이 공통의 콘텐츠 키의 설정이 가능하다. 또한, 새로운 콘텐츠 키 Kcon을 노드 키 K00으로 암호화한 값 Enc(K00, Kcon)을, 네트워크를 통해 혹은 기록 매체에 저장하여 디바이스 0, 1, 2, 3에 배포하면, 디바이스 0, 1, 2, 3만이, 각각의 디바이스에서 보유하는 공유 노드 키 K00을 이용하여 암호 Enc(K00, Kcon)를 풀어 콘텐츠 키 Kcon을 얻는 것이 가능해진다. 또, Enc(Ka, Kb)는 Kb를 Ka에 의해서 암호화한 데이터임을 나타낸다.

또한, 어느 시점 t에 있어서, 디바이스 3이 소유하는 키 K0011, K001, K00, K0, KR이 공격자(해커)에 의해 해석되어 노출된 것이 발각된 경우, 그 이후, 시스템(디바이스 0, 1, 2, 3의 그룹)에서 송수신되는 데이터를 보호하기 위해서, 디바이스 3을 시스템으로부터 분리할 필요가 있다. 이를 위해서는, 노드 키 K001, K00, K0, KR을 각각 새로운 키 K(t)001, K(t)00, K(t)0, K(t)R로 갱신하고, 디바이스 0, 1, 2에 그 갱신 키를 전달할 필요가 있다. 여기서, K(t)aaa는 키 Kaaa의 세대(Generation) t의 갱신 키임을 나타낸다.

갱신 키의 배포 처리 대하여 설명한다. 키의 갱신은 예를 들면, 도 15A에 도시한 유효화 키 블록(EKB: Enabling Key Block)이라 불리는 블록 데이터로 구성되는 테이블을, 네트워크를 통해 혹은 기록 매체에 저장하여 디바이스 0, 1, 2에 공급함으로써 실행된다. 또, 유효화 키 블록(EKB)은 도 12에 도시한 바와 같은 트리 구조를 구성하는 각 리프(최하단의 노드)에 대응하는 디바이스에, 새롭게 갱신된 키를 배포하기 위한 암호화 키에 의해서 구성된다. 유효화 키 블록(EKB)은 키 갱신 블록(KRB: Key Renewal Block)이라고 불리는 경우도 있다.

도 15A에 도시한 유효화 키 블록(EKB)은, 노드 키의 갱신이 필요한 디바이스만이 갱신 가능한 데이터 구성을 갖는 블록 데이터로서 구성된다. 도 15A의 예는, 도 12에 도시한 트리 구조 중의 디바이스 0, 1, 2에 있어서, 세대 t의 갱신 노드 키를 배포하는 것을 목적으로 하여 형성된 블록 데이터이다. 도 12로부터 분명한 바와 같이, 디바이스 0과 디바이스 1은 갱신 노드 키로서 K(t)00, K(t)0, K(t)R이 필요하고, 디바이스 2는 갱신 노드 키로서 K(t)001, K(t)00, K(t)0, K(t)R이 필요하다.

도 15A의 EKB에 도시한 바와 같이, EKB에는 복수의 암호화 키가 포함된다. 도 15A의 최하단의 암호화 키는 Enc(K0010, K(t)001)이다. 이것은 디바이스 2가 갖는 리프 키 K0010에 의해서 암호화된 갱신 노드 키 K(t)001이고, 디바이스 2는 자신이 갖는 리프 키 K0010에 의해서 이 암호화 키를 복호하여, 갱신 노드 키 K(t)001을 얻을 수 있다. 또한, 복호에 의해 얻은 갱신 노드 키 K(t)001을 이용하여, 도 15A의 아래서부터 2단째의 암호화 키 Enc(K(t)001, K(t)00)가 복호 가능해져, 갱신 노드 키 K(t)00을 얻을 수 있다.

이하 순차적으로, 도 15A의 위로부터 2단째의 암호화 키 Enc(K(t)00, K(t)0)를 복호함으로써, 갱신 노드 키 K(t)0이 얻어지고, 이것을 이용하여, 도 15A의 위로부터 1단째의 암호화 키 Enc(K(t)0, K(t)R)를 복호함으로써, 갱신 루트 키 K(t)R이 얻어진다.

한편, 노드 키 K000은 갱신할 대상에 포함되어 있지 않으며, 노드(0, 1)가 갱신 노드 키로서 필요한 것은 K(t)00, K(t)0, K(t)R이다. 노드(0, 1)는 디바이스 노드 키에 포함되는 노드 키 K000을 이용하여, 도 15A의 위로부터 3단째의

암호화 키 Enc(K000, K(t)00)를 복호함으로써 갱신 노드 키 K(t)00을 취득하고, 이하 순차적으로 도 15A의 위로부터 2단째의 암호화 키 Enc(K(t)00, K(t)0)를 복호함으로써, 갱신 노드 키 K(t)0을 얻고, 도 15A의 위로부터 1단째의 암호화 키 Enc(K(t)0, K(t)R)를 복호함으로써, 갱신 루트 키 K(t)R을 얻는다. 이와 같이 하여, 디바이스 0, 1, 2는 갱신된 키 K(t)R을 얻을 수 있다.

또, 도 15A의 인덱스는 도면 우측의 암호화 키를 복호하기 위한 복호 키로서 사용하는 노드 키, 리프 키의 절대 번지를 나타낸다.

도 12에 도시한 트리 구조의 상위단의 노드 키 K(t)0, K(t)R의 갱신이 불필요하고, 노드 키 K00만의 갱신 처리가 필요한 경우에는, 도 15B의 유효화 키 블록(EKB)을 이용함으로써, 갱신 노드 키 K(t)00을 디바이스 0, 1, 2에 배포할 수 있다.

도 15B에 도시한 EKB는, 예를 들면 특정한 그룹에서 공유하는 새로운 콘텐츠 키를 배포하는 경우에 이용 가능하다. 구체예로서, 도 12에 점선으로 표시된 그룹 내의 디바이스 0, 1, 2, 3이 있는 기록 매체를 이용하고 있고, 새로운 공통의 콘텐츠 키 K(t)con이 필요하다고 한다. 이 때, 디바이스 0, 1, 2, 3의 공통의 노드 키 K00을 갱신한 K(t)00을 이용하여 새로운 공통의 갱신 콘텐츠 키 K(t)con을 암호화한 데이터 Enc(K(t)00, K(t)con)가, 도 15B에 도시한 EKB와 함께 배포된다. 이 배포에 의해, 디바이스 4 등 그 밖의 그룹 기기가 복호할 수 없는 데이터로서의 배포가 가능해진다.

즉, 디바이스 0, 1, 2는 EKB를 처리하여 얻은 키 K(t)00을 이용하여 암호문을 복호하면, t 시점에서의 콘텐츠 키 K(t)con을 얻는 것이 가능하게 된다.

도 16에, t 시점에서의 콘텐츠 키 K(t)con을 얻는 처리예로서, K(t)00을 이용하여 새로운 공통의 콘텐츠 키 K(t)con을 암호화한 데이터 Enc(K(t)00, K(t)con)와, 도 15B에 도시한 EKB를 기록 매체를 통해 수령한 디바이스 0의 처리를 도시한다. 즉, 이 예는 EKB에 의한 암호화 메시지 데이터를 콘텐츠 키 K(t)con으로 한 예이다.

도 16에 도시한 바와 같이, 디바이스 0은 기록 매체에 저장되어 있는 세대 t 시점의 EKB와, 자신이 미리 저장하고 있는 DNK에 포함되는 노드 키 K000을 이용하여, 상술한 경우와 마찬가지의 EKB 처리에 의해 노드 키 K(t)00을 생성한다. 또한, 디바이스 0은 복호한 갱신 노드 키 K(t)00을 이용하여, 갱신 콘텐츠 키 K(t)con을 복호하고, 후에 그것을 사용하기 위해서 자신만이 갖는 리프 키 K0000으로 암호화하여 저장한다.

도 17에 유효화 키 블록(EKB)의 포맷예를 도시한다. 버전(601)은 유효화 키 블록(EKB)의 버전을 도시하는 식별자이다. 또, 버전은 최신의 EKB를 식별하는 기능과, 콘텐츠와의 대응 관계를 나타내는 기능을 갖는다. 뎁스는 유효화 키 블록(EKB)의 배포처의 디바이스에 대한 계층 트리의 계층 수를 나타낸다. 데이터 포인터(603)는 유효화 키 블록(EKB) 내의 데이터부(606)의 위치를 나타내는 포인터이고, 태그 포인터(604)는 태그부(607)의 위치, 서명 포인터(605)는 서명(608)의 위치를 나타내는 포인터이다.

데이터부(606)는 예를 들면 갱신하는 노드 키를 암호화한 데이터를 저장한다. 예를 들면 도 16에 도시한 바와 같은 갱신된 노드 키에 관한 각 암호화 키 등을 저장한다.

태그부(607)는 데이터부(606)에 저장된 암호화된 노드 키, 리프 키의 위치 관계를 나타내는 태그이다. 이 태그의 부여를 도 18을 이용하여 설명한다.

도 18에서는 데이터로서 앞서 도 15A에서 설명한 유효화 키 블록(EKB)을 송부하는 예를 도시하고 있다. 이 때의 데이터는 도 18의 테이블에 도시한 바와 같이 된다. 이 때의 암호화 키에 포함되는 톱 노드의 어드레스를 톱 노드 어드레스

로 한다. 이 예의 경우에는 루트 키의 갱신 키 K(t)R이 포함되어 있기 때문에, 톱 노드 어드레스는 KR이 된다. 이 때, 예를 들면 최상단의 데이터 Enc(K(t)0, K(t)R)는, 도 18에 도시한 계층 트리에 도시한 위치 P0에 대응한다. 다음 단의 데이터는 Enc(K(t)00, K(t)0)이고, 트리 상에서는 앞 데이터의 좌측 아래의 위치 P00에 대응한다. 트리 구조의 소정의 위치에서 보아, 그 아래에 데이터가 있는 경우에는, 태그가 0, 없는 경우에는 태그가 1로 설정된다. 태그는 {좌측(L) 태그, 우측(R) 태그}로서 설정된다. 도 18의 테이블 최상단의 데이터 Enc(K(t)0, K(t)R)에 대응하는 위치 P0의 좌측 아래의 위치 P00에는 데이터가 있기 때문에, L 태그=0, 우측에는 데이터가 없기 때문에, R 태그=1이 된다. 이하, 모든 데이터에 태그가 설정되고, 도 18에 도시한 데이터 열 및 태그 열이 구성된다.

태그는 대응하는 데이터 Enc(Kxxx, Kyyy)가 트리 구조의 어디에 위치하고 있는 것인지를 나타내기 위해서 설정되는 것이다. 데이터부(606)에 저장되는 키 데이터 Enc(Kxxx, Kyyy)…는, 단순하게 암호화된 키의 나열 데이터에 불과하지만, 상술한 태그에 의해서 데이터로서 저장된 암호화 키의 트리 상의 위치가 판별 가능해진다. 상술한 태그를 이용하지 않고서, 앞의 도 15A 및 도 15B에서 설명한 구성과 같이, 암호화 데이터에 대응시킨 노드 인덱스를 이용하여, 예를 들면,

0: Enc(K(t)0, K(t)R)

00: Enc(K(t)00, K(t)0)

000: Enc(K((t)000, K(t)00)

…와 같은 데이터 구성으로 하는 것도 가능하지만, 이러한 인덱스를 이용한 구성으로 하면, 용장 데이터가 되어 데이터량이 증대되어, 네트워크를 통하는 배신 등에서는 바람직하지 못하다. 이에 대하여, 상술한 태그를 키 위치를 나타내는 색인 데이터로서 이용함으로써, 적은 데이터 량으로 키 위치의 판별이 가능해진다.

도 17로 되돌아가, EKB 포맷에 대하여 더 설명한다. 서명(Signature)(608)은 유효화 키 블록(EKB)을 발행한 예를 들면 키 관리 센터(라이센스 서버(4)), 콘텐츠 프로바이더(콘텐츠 서버(3)), 결제 기관(과금 서버(5)) 등이 실행하는 전자 서명이다. EKB를 수령한 디바이스는 서명 검증에 의해서 정당한 유효화 키 블록(EKB) 발행자가 발행한 유효화 키 블록(EKB)이라는 것을 확인한다.

이상과 같이 하여, 라이센스 서버(4)로부터 공급된 라이센스에 기초하여, 콘텐츠 서버(3)로부터 공급된 콘텐츠를 이용하는 처리를 정리하면, 도 19에 도시한 바와 같이 된다.

즉, 콘텐츠 서버(3)로부터 클라이언트(1)에 대하여 콘텐츠가 제공됨과 함께, 라이센스 서버(4)로부터 클라이언트(1)에 대하여 라이센스가 제공된다. 콘텐츠는 콘텐츠 키 Kc에 의해 암호화되어 있고(Enc(Kc, Content)), 콘텐츠 키 Kc는 루트 키 KR(EKB로부터 얻어지는 키이고, 도 5에서의 키 K_{EKBC} 에 대응함)로 암호화되고(Enc(KR, Kc)), EKB와 함께, 암호화된 콘텐츠에 부가되어 클라이언트(1)에 제공된다.

도 19의 예에서의 EKB에는 예를 들면, 도 20에 도시한 바와 같이, DNK로 복호 가능한 루트 키 KR이 포함되어 있다(Enc(DNK, KR)). 따라서, 클라이언트(1)는 서비스 데이터에 포함되는 DNK를 이용하여, EKB로부터 루트 키 KR을 얻을 수 있다. 또한, 루트 키 KR을 이용하여 Enc(KR, Kc)로부터 콘텐츠 키 Kc를 복호할 수 있고, 콘텐츠 키 Kc를 이용하여 Enc(Kc, Content)로부터 콘텐츠를 복호할 수 있다.

이와 같이, 클라이언트(1)에 DNK를 개별로 할당함으로써, 도 12, 및 도 15A와 도 15B를 참조하여 설명한 원리에 따라서, 개개의 클라이언트(1)의 리보크(revoke)가 가능해진다.

또한, 라이센스에 리프 ID를 부가하여 배포함으로써, 클라이언트(1)에 있어서, 서비스 데이터와 라이센스의 대응이 이루어지게 되어, 라이센스의 부정 복사를 방지하는 것이 가능해진다.

또한, 클라이언트용의 증명서와 비밀 키를 서비스 데이터로서 배신하도록 함으로써, 마지막 사용자도 이들을 이용하여 부정 복사가 방지 가능한 콘텐츠를 작성하는 것이 가능해진다.

증명서와 비밀 키의 이용에 대해서는 도 29의 흐름도를 참조하여 후술한다.

본 발명에서는 도 13을 참조하여 설명한 바와 같이, 카테고리 노드에 라이센스를 관리하는 본 발명의 콘텐츠 배신 시스템과, 각종 콘텐츠를 이용하는 디바이스의 카테고리를 대응시키므로, 복수의 DNK를 동일 디바이스에 갖게 할 수 있다. 그 결과, 서로 다른 카테고리의 콘텐츠를 하나의 디바이스로 관리하는 것이 가능해진다.

도 21은 이 관계를 도시하고 있다. 즉, 디바이스 D1에는 콘텐츠 배신 시스템에 기초하여 DNK1이 할당되어 있다. 콘텐츠 1을 이용하는 라이센스 및 서비스 데이터가 기록된다. 마찬가지로, 이 디바이스 D1에는 예를 들면, DNK2가 할당된, 메모리스틱에 CD로부터 립핑한 콘텐츠 2를 기록할 수 있다. 이 경우, 디바이스 D1은 콘텐츠 1과 콘텐츠 2라고 하는, 서로 다른 시스템(콘텐츠 배신 시스템과 디바이스 관리 시스템)에 의해 배신된 콘텐츠를 동시에 처리하는 것이 가능해진다. 새로운 DNK를 할당할 때, 이미 할당되어 있는 DNK를 삭제하는 등으로 하여 디바이스에 하나의 DNK만을 대응시키도록 한 경우, 이와 같은 것은 불가능하다.

또한, 도 13에서의, 예를 들면 하측 32계층의 각 삼각형의 하나 하나에, 도 22에 도시한 라이센스 카테고리 1과 라이센스 카테고리 2를 할당함으로써, 동일 카테고리 내를 서브 카테고리를 이용하여, 콘텐츠의 장르, 레벨, 판매점, 배신 서비스, 콘텐츠의 출처, 제공 방법 등의 작은 집합으로 분류하여 관리하는 것이 가능해진다.

도 22의 예에서는 예를 들면, 라이센스 카테고리 1은 재즈 장르에 속하고, 라이센스 카테고리 2는 락 장르에 속한다. 라이센스 카테고리 1에는 라이센스 ID가 1인 콘텐츠 1과 콘텐츠 2를 대응시키고, 각각 사용자 1 내지 사용자 3에 배포되어 있다. 라이센스 카테고리 2는 라이센스 ID2의 콘텐츠 3, 콘텐츠 4, 및 콘텐츠 5가 포함되고, 각각 사용자 1과 사용자 3에 제공되어 있다.

이와 같이, 본 발명에서는 카테고리마다 독립된 키 관리가 가능해진다.

또한, DNK를 기기나 미디어에 미리 매립하는 것이 아니라, 라이센스 서버(4)에 의해 등록 처리를 행할 때에 각 기기나 미디어에 다운로드하도록 함으로써, 사용자에 의한 키의 취득이 가능한 시스템을 실현할 수 있다.

이 경우의 클라이언트(1)의 등록 처리에 대하여 도 23을 참조하여 설명한다.

단계 S161에 있어서, 클라이언트(1)의 CPU(21)는 통신부(29)를 제어하여 라이센스 서버(4)에 서비스 데이터 요구를 송신한다. 라이센스 서버(4)의 CPU(21)는 단계 S165에 있어서, 통신부(29)를 통하여 입력되는 서비스 데이터 요구를 수신하면, S166에 있어서, 통신부(29)를 통하여 사용자 정보 요구를 클라이언트(1)에 송신한다.

클라이언트(1)의 CPU(21)는 단계 S162에 있어서, 통신부(29)를 통해서 사용자 정보 요구를 수신하면, 출력부(27)를 제어하여 디스플레이 등에 사용자 정보의 입력을 재촉하는 메시지를 표시시킨다. 사용자가 키보드 등을 조작함으로써, 입력부(26)로부터 사용자 본인의 개인 정보나 결제 정보 등의 사용자 정보를 입력하면, S163에 있어서, 클라이언트(1)의 CPU(21)는 입력된 사용자 정보를 통신부(29)를 통해서 라이센스 서버(4)에 송신한다.

라이센스 서버(4)의 CPU(21)는 단계 S167에 있어서, 통신부(29)를 통해서 사용자 정보를 수신하면, 단계 S168에 있어서, 그 라이센스 서버(4)에 할당된 카테고리의 노드 이하의 리프 중, 아직 할당되어 있지 않은 리프를 클라이언트(1)에 할당하고, 그 리프로부터 라이센스 서버(4)에 할당된 카테고리의 노드까지의 패스 상의 노드에 할당된 노드 키의 조를 디바이스 노드 키로서 생성하고, 생성된 디바이스 노드 키, 클라이언트(1)에 할당된 리프의 리프 ID, 클라이언트(1)의 비밀 키, 클라이언트(1)의 비밀 키· 공개 키의 쌍, 라이센스 서버의 공개 키, 및 각 공개 키의 증명서를 통합하여 서비스 데이터로서 생성하고, S169에 있어서 통신부(29)를 통하여 클라이언트에 생성된 서비스 데이터를 송신함

과 함께, 드라이브(30)를 제어하여 사용자 정보를 리프 ID와 대응시켜서 하드디스크 등의 기록 미디어에 기록시킨다.

클라이언트(1)의 CPU(21)는 단계 S164에 있어서, 통신부(29)를 통하여 서비스 데이터를 수신하면, 암호화 복호부(24)를 제어하여 수신한 서비스 데이터를 암호화하고, 드라이브(30)를 제어하여 하드디스크 등의 기록 미디어에 기록시킨다.

이상과 같이 하여, 라이센스 서버(4)는 클라이언트(1) 및 그 사용자를 등록하고, 클라이언트(1)는 소망의 콘텐츠 배신 서비스를 이용하기 위해서 필요한, 디바이스 노드 키를 포함하는 서비스 데이터를 수취할 수 있다.

콘텐츠는 그것이 작성된 후, 어떠한 사용 방법을 쓰더라도, 그 사용 방법에 상관없이 모든 용도에 있어서 사용 가능한 것이 바람직하다. 예를 들면, 서로 다른 콘텐츠 배신 서비스 혹은 도메인 사용 상황이 다른 경우에 있어서도, 동일한 콘텐츠를 사용할 수 있는 것이 바람직하다. 본 발명에서는 이를 위해, 상술한 바와 같이, 각 사용자(클라이언트(1))에게 인증국으로서의 라이센스 서버(4)로부터 비밀 키와 그것에 대응하는 공개 키의 증명서(certificates)가 배포된다. 각 사용자는 그 비밀 키를 이용하여 서명(signature)을 작성하고, 콘텐츠에 부가하여, 콘텐츠의 진정성(integrity)을 보증하고, 또한 콘텐츠의 개찬(改竄) 방지를 도모할 수 있다.

이 경우의 처리예에 대하여, 도 24의 흐름도를 참조하여 설명한다. 도 24의 처리는 사용자가 CD로부터 재생된 데이터를 기억부(28)에 기억시키는 립핑 처리를 설명하는 것이다.

처음에, 단계 S171에 있어서, 클라이언트(1)의 CPU(21)는 통신부(29)를 통해서 입력되는 CD의 재생 데이터를 기록 데이터로서 취득한다. 단계 S172에 있어서, CPU(21)는 단계 S171의 처리에서 취득된 기록 데이터에 워터마크가 포함되어 있는지의 여부를 판정한다. 이 워터마크는 3비트의 복사 관리 정보(CCI)와 1비트의 트리거(Trigger)로 구성되고, 콘텐츠의 데이터 내에 매립되어 있다. CPU(21)는 워터마크가 검출되었을 경우에는, 단계 S173으로 진행하여, 그 워터마크를 추출하는 처리를 실행한다. 워터마크가 존재하지 않는 경우에는, 단계 S173의 처리는 스킵된다.

다음에, 단계 S174에 있어서, CPU(21)는 콘텐츠에 대응하여 기록하는 헤더의 데이터를 작성한다. 이 헤더의 데이터는 콘텐츠 ID, 라이센스 ID, 라이센스를 취득하기 위한 액세스처를 나타내는 URL, 및 워터마크에 포함되어 있는 복사 관리 정보(CCI)와, 트리거(Trigger)로 구성된다.

다음에, 단계 S175로 진행하여, CPU(21)는 단계 S174의 처리에서 작성한 헤더의 데이터에 기초한 디지털 서명을, 자기 자신의 비밀 키를 이용하여 작성한다. 이 비밀 키는 라이센스 서버(4)로부터 취득한 것이다(도 7의 단계 S67).

단계 S176에서, CPU(21)는 암호화 복호부(24)를 제어하고, 콘텐츠 키로 콘텐츠를 암호화시킨다. 콘텐츠 키는 난수 등을 이용하여 생성된다.

다음에, 단계 S177에 있어서, CPU(21)는 파일 포맷에 기초하여, 데이터를 예를 들면 미니 디스크 등으로 구성되는 광자기 디스크(43)에 기록시킨다.

또, 기록 매체가 미니 디스크인 경우, 단계 S176에 있어서, CPU(21)는 콘텐츠를 코덱부(25)에 공급하여, 예를 들면, ATRAC3 방식에 의해 콘텐츠를 부호화시킨다. 그리고, 부호화된 데이터가 암호화 복호부(24)에 의해 더 암호화된다.

도 25는 이상과 같이 하여, 기록 매체에 콘텐츠가 기록된 상태를 모식적으로 도시하고 있다. 암호화되어 있는 콘텐츠(E(At3))로부터 추출된 워터마크(WM)가, 콘텐츠의 밖(헤더)에 기록되어 있다.

도 26은 콘텐츠를 기록 매체에 기록하는 경우의 파일 포맷의 보다 상세한 구성을 도시하고 있다. 이 예에서는 콘텐츠 ID(CID), 라이센스 ID(LID), URL, 및 워터마크(WM)를 포함하는 헤더가 기록되어 있는 외에, EKB, 콘텐츠 키 Kc를 루트 키 KR로 암호화한 데이터(Enc(KR, Kc)), 증명서(Cert), 헤더에 기초하여 생성된 디지털 서명(Sig(Header)), 콘텐츠를 콘텐츠 키 Kc로 암호화한 데이터(Enc(Kc, Content)), 메타 데이터(Meta Data) 및 마크(Mark)가 기록되어 있다.

워터마크는 콘텐츠의 내부에 매립되어 있는 것이지만, 도 25와 도 26에 도시한 바와 같이, 콘텐츠의 내부와는 별도로 헤더 내에 배치하도록 함으로써, 워터마크로서 콘텐츠에 매립되어 있는 정보를 신속하면서도 간단히 검출하는 것이 가능해진다. 따라서, 그 콘텐츠를 복사할 수 있는지의 여부를 신속하게 판정할 수 있다.

또, 메타 데이터는 예를 들면 재킷, 사진, 가사 등의 데이터를 나타낸다. 마크에 대해서는 도 32를 참조하여 후술한다.

도 27은 증명서로서의 공개 키 증명서의 예를 도시하고 있다. 공개 키 증명서는 통상적으로 공개 키 암호 방식에서의 인증국(CA: Certificate Authority)이 발행하는 증명서이며, 사용자가 인증국에 제출한 자기의 ID나 공개 키 등에, 인증국이 유효 기한 등의 정보를 부가하고, 또한 인증국에 의한 디지털 서명을 부가하여 작성된다. 본 발명에서는 라이센스 서버(4)(또는 콘텐츠 서버(5))가 증명서와 비밀 키, 그에 따른 공개 키도 발행하기 때문에, 사용자는 사용자 ID, 패스워드 등을 라이센스 서버(4)에 제공하여 등록 처리를 행함으로써, 이 공개 키 증명서를 얻을 수 있다.

도 27에서의 공개 키 증명서는, 증명서의 버전 번호, 라이센스 서버(4)가 증명서의 이용자(사용자)에 대하여 할당하는 증명서의 일련 번호, 디지털 서명에 이용한 알고리즘 및 파라미터, 인증국(라이센스 서버(4))의 이름, 증명서의 유효 기한, 증명서 이용자의 ID(노드 ID 또는 리프 ID), 및 증명서 이용자의 공개 키가, 메시지로서 포함되어 있다. 또한, 이 메시지에는 인증국으로서의 라이센스 서버(4)에 의해 작성된 디지털 서명이 부가되어 있다. 이 디지털 서명은 메시지에 대하여 해시 함수를 적용하여 생성된 해시값에 기초하여, 라이센스 서버(4)의 비밀 키를 이용하여 생성된 데이터이다.

노드 ID 또는 리프 ID는 예를 들면, 도 12의 예의 경우, 디바이스 0이면 「0000」으로 되고, 디바이스 1이면 「0001」로 되고, 디바이스 15이면 「1111」로 된다. 이러한 ID에 기초하여, 그 디바이스(엔티티)가 트리 구성의 어떤 위치(리프 또는 노드)에 위치하는 것인지가 식별된다.

이와 같이, 콘텐츠를 이용하는 데 필요한 라이센스를 콘텐츠와는 분리하여 배포하도록 함으로써, 콘텐츠의 배포가 자유롭게 행해지게 된다. 임의의 방법 혹은 임의의 경로로 입수된 콘텐츠는 일원적으로 처리하는 것이 가능하다.

또한, 파일 포맷을 도 26에 도시한 바와 같이 구성함으로써, 그 포맷의 콘텐츠를 인터넷을 통해 배신하는 경우는 물론, SDMI(Secure Digital Music Initiative) 기기에 제공하는 경우에도 콘텐츠의 저작권을 관리하는 것이 가능해진다.

또한, 예를 들면 도 28에 도시한 바와 같이, 콘텐츠가 기록 매체를 통해 제공되었다고 하여도, 인터넷(2)을 통해 제공되었다고 하여도, 마찬가지 처리에 의해 SDMI(Secure Digital Music Initiative) 기기로서의 소정의 PD(Portable Device) 등에 체크아웃하는 것이 가능해진다.

다음에, 도 29의 흐름도를 참조하여, 클라이언트(1)가 다른 클라이언트(예를 들면, PD)에 대하여 콘텐츠를 체크아웃하는 경우의 처리에 대하여 설명한다.

처음에, 단계 S191에 있어서, CPU(21)는 콘텐츠에 디지털 서명이 부가되어 있는지의 여부를 판정한다. 디지털 서명이 부가되어 있다고 판정된 경우, 단계 S192로 진행하고, CPU(21)는 증명서를 추출하여, 인증국(라이센스 서버(4))의

공개 키로 검증하는 처리를 실행한다. 즉, 클라이언트(1)는 라이센스 서버(4)로부터 라이센스 서버(4)의 비밀 키에 대응하는 공개 키를 취득하고, 그 공개 키로 공개 키 증명서에 부가되어 있는 디지털 서명을 복호한다. 도 27을 참조하여 설명한 바와 같이, 디지털 서명은 인증국(라이센스 서버(4))의 비밀 키에 기초하여 생성되어 있고, 라이센스 서버(4)의 공개 키를 이용하여 복호할 수 있다. 또한, CPU(21)는 증명서의 메시지 전체에 대하여 해시 함수를 적용하여 해시값을 연산한다. 그리고 CPU(21)는, 연산된 해시값과, 디지털 서명을 복호하여 얻어진 해시값을 비교하여, 양자가 일치하면, 메시지는 개찬된 것이 아니라고 판정한다. 양자가 일치하지 않는 경우에는, 이 증명서는 개찬된 것이라고 판정한다.

따라서, 단계 S193에 있어서, CPU(21)는, 증명서가 개찬되어 있지 않은지의 여부를 판정하고, 개찬되어 있지 않다고 판정된 경우, 단계 S194로 진행하여, 증명서를 EKB로 검증하는 처리를 실행한다. 이 검증 처리는 증명서에 포함되는 리프 ID(도 27)에 기초하여, EKB를 찾아갈 수 있는지의 여부를 조사함으로써 행해진다. 이 검증에 대하여 도 30과 도 31을 참조하여 설명한다.

지금, 도 30에 도시한 바와 같이, 예를 들면, 리프 키 K1001을 갖는 디바이스가 리보크된 디바이스라고 한다. 이 때, 도 31에 도시한 바와 같은 데이터(암호화 키)와 태그를 갖는 EKB가 각 디바이스(리프)에 배포된다. 이 EKB는 도 30에서의 디바이스 「1001」을 리보크하기 위해서, 키 KR, K1, K10, K100을 갱신하는 EKB로 되어 있다.

리보크 디바이스 「1001」 이외의 모든 리프는, 갱신된 루트 키 K(t)R을 취득할 수 있다. 즉, 노드 키 K0의 하위에 연속해 있는 리프는, 갱신되어 있지 않은 노드 키 K0을 디바이스 내에 보유하고 있기 때문에, 암호화 키 Enc(K0, K(t)R)를 키 K0에 의해서 복호함으로써, 갱신 루트 키 K(t)R을 취득할 수 있다.

또한, 노드(11) 이하의 리프는, 갱신되어 있지 않은 노드 키 K11을 이용하여, Enc(K11, K(t)1)를 노드 키 K11에 의해서 복호함으로써, 갱신 노드 키 K(t)1을 취득할 수 있다. 또한, Enc(K(t)1, K(t)R)를 노드 키 K(t)1에 의해서 복호함으로써, 갱신 루트 키 K(t)R을 취득하는 것이 가능해진다. 노드 키 K101의 하위 리프에 대해서도 마찬가지로 갱신 루트 키 K(t)R을 취득하는 것이 가능하다.

또한, 리보크되어 있지 않은 리프 키 K1000을 갖는 디바이스 「1000」은, 자기의 리프 키 K1000으로 Enc(K1000, K(t)100)를 복호하여 노드 키 K(t)100을 취득할 수 있고, 이것을 이용하여 또한, 상위의 노드 키를 순차적으로 복호하여 갱신 루트 키 K(t)R을 취득할 수 있다.

이에 대하여, 리보크된 디바이스 「1001」은, 자기 리프의 1단 위의 갱신 노드 키 K(t)100을 EKB 처리에 의해 취득할 수 없기 때문에, 결국 갱신 루트 키 K(t)R을 취득할 수 없다.

리보크되어 있지 않은 정당한 디바이스(클라이언트(1))에는, 도 31에 도시한 데이터와 태그를 갖는 EKB가 라이센스 서버(4)로부터 배신되어 저장되어 있다.

따라서, 각 클라이언트는 그 태그를 이용하여 EKB 추적 처리를 행할 수 있다. 이 EKB 추적 처리는 상위의 루트 키로부터 키 배신 트리를 찾아갈 수 있는지의 여부를 판정하는 처리이다.

예를 들면, 도 30의 리프 「1001」의 ID(리프 ID)인 「1001」을 「1」 「0」 「0」 「1」의 4 비트로서 파악하고, 최상위 비트로부터 순차적으로 하위 비트에 따라서 트리를 찾아갈 수 있는지의 여부가 판정된다. 이 판정에서는 비트가 1이면, 우측으로 진행하고, 0이면 좌측으로 진행하는 처리가 행해진다.

ID 「1001」의 최상위 비트가 1이기 때문에, 도 30의 루트 키 KR로부터 우측으로 진행한다. EKB의 최초의 태그(번호 0의 태그)는 0:{0, 0}이고, 양 브랜치에 데이터를 갖는 것이라고 판정된다. 이 경우, 우측으로 진행할 수 있기 때문에, 노드 키 K1에 도착할 수 있다.

다음에, 노드 키 K1의 하위 노드로 진행한다. ID 「1001」의 2번째 비트는 0이기 때문에 좌측으로 진행한다. 번호 1의 태그는 좌측의 노드 키 K0의 하위 데이터의 유무를 나타내는 것이고, 노드 키 K1의 하위 데이터의 유무를 나타내는 태그는, 번호 2의 태그이다. 이 태그는 도 31에 도시한 바와 같이, 2:{0, 0}이고, 양 브랜치에 데이터를 갖게 된다. 따라서, 좌측으로 진행하여, 노드 키 K10에 도착할 수 있다.

또한, ID 「1001」의 3번째 비트는 0이고, 좌측으로 진행한다. 이 때, K10의 하위 데이터의 유무를 나타내는 태그(번호 3의 태그)는 3:{0,0}이고, 양 브랜치에 데이터를 갖는 것으로 판정된다. 따라서, 좌측으로 진행하여, 노드 키 K100에 도착할 수 있다.

또한, ID 「1001」의 최하위 비트는 1이고, 우측으로 진행한다. 번호 4의 태그는 노드 키 K11에 대응하는 것이고, K100의 하위 데이터의 부호를 나타내는 태그는 번호 5의 태그이다. 이 태그는 5:{0, 1}이다. 따라서, 우측에는 데이터가 존재하지 않게 된다. 그 결과, 노드 「1001」에는 도착하지 못하게 되어, ID 「1001」의 디바이스는 EKB에 의한 갱신 루트 키를 취득할 수 없는 디바이스, 즉 리보크 디바이스라고 판정된다.

이에 대하여, 예를 들면, 리프 키 K1000을 갖는 디바이스 ID는 「1000」이고, 상술한 경우와 마찬가지로, EKB 내의 태그에 기초하는 EKB 추적 처리를 행하면, 노드 「1000」에 도착할 수 있다. 따라서, ID 「1000」의 디바이스는 정당한 디바이스라고 판정된다.

도 29로 되돌아가, CPU(21)는 단계 S194의 검증 처리에 기초하여, 증명서가 리보크되어 있지 않은지의 여부를 단계 S195에서 판정하고, 증명서가 리보크되어 있지 않은 경우에는, 단계 S196으로 진행하여, 디지털 서명을 증명서에 포함되는 공개 키로 검증하는 처리를 실행한다.

즉, 도 27에 도시한 바와 같이, 증명서에는 증명서 이용자(콘텐츠 작성자)의 공개 키가 포함되어 있고, 이 공개 키를 이용하여 도 26에 도시한 서명(Sig(Header))이 검증된다. 즉, 이 공개 키를 이용하여, 디지털 서명 Sig(Header)를 복호하여 얻어진 데이터(해시값)와, 도 26에 도시한 Header에 해시 함수를 적용하여 연산된 해시값을 비교함으로써, 양자가 일치하면, Header가 개찬되어 있지 않다는 것을 확인할 수 있다. 이에 대하여, 양자가 일치하지 않으면, Header는 개찬되어 있는 것으로 된다.

단계 S197에 있어서, CPU(21)는 Header가 개찬되어 있는지의 여부를 판정하고, 개찬되어 있지 않으면, 단계 S198로 진행하여, 워터마크를 검증한다. 단계 S199에 있어서, CPU(21)는 워터마크의 검증 결과, 체크아웃이 가능인지의 여부를 판정한다. 체크아웃이 가능한 경우에는, 단계 S200으로 진행하여, CPU(21)는 체크아웃을 실행한다. 즉, 체크아웃처의 클라이언트(1)에 대하여 콘텐츠를 전송하여 복사시킨다.

단계 S191에서 디지털 서명이 존재하지 않는다고 판정된 경우, 단계 S193에서 증명서가 개찬되어 있다고 판정된 경우, 단계 S195에서 증명서를 EKB에서 검증할 수 없었다고 판정된 경우, 단계 S197에서 디지털 서명의 검증 결과, 헤더가 개찬되어 있다고 판정된 경우, 또는 단계 S199에서 워터마크에 체크아웃 금지가 기술되어 있다고 판정된 경우, 단계 S201로 진행하여, 에러 처리가 실행된다. 즉, 이 경우에는 체크아웃이 금지된다.

이와 같이, 증명서와 비밀 키를 라이센스 서버(4)로부터 사용자에게 배포하고, 콘텐츠 작성 시에, 디지털 서명을 부가함으로써, 콘텐츠의 작성자의 진정성을 보증하는 것이 가능해진다. 이에 의해, 부정한 콘텐츠의 유통을 억제할 수 있다.

또한, 워터마크를 콘텐츠 작성 시에 검출하고, 그 정보를 디지털 서명에 첨부함으로써, 워터마크 정보의 개찬을 방지하여 콘텐츠의 진정성을 보증할 수 있다.

그 결과, 한번 작성된 콘텐츠는 어떠한 형태로 배신되었다고 하여도, 원래의 콘텐츠의 진정성을 보증하는 것이 가능해진다.

또한, 콘텐츠는 사용 조건을 갖지 않고, 사용 조건은 라이센스에 부가되어 있기 때문에, 라이센스 내의 사용 조건을 변경함으로써, 그것에 관계된 콘텐츠의 사용 조건을 일제히 변경하는 것이 가능해진다.

다음에, 마크의 이용 방법에 대하여 설명한다. 본 발명에서는 상술한 바와 같이, 사용 조건은 콘텐츠가 아니라, 라이센스에 부가된다. 그러나, 콘텐츠에 따라서 사용 상황이 다른 경우가 있다. 따라서, 본 발명에서는 도 26에 도시한 바와 같이 콘텐츠에 마크가 부가된다.

라이센스와 콘텐츠는 일대다수의 관계에 있기 때문에, 콘텐츠 개개의 사용 상황을 라이센스의 사용 조건에만 기술하는 것은 곤란해진다. 따라서, 이와 같이 콘텐츠에 사용 상황을 부가함으로써, 라이센스에서의 관리를 하면서도 개개의 콘텐츠를 관리하는 것이 가능해진다.

이 마크에는 예를 들면, 도 32에 도시한 바와 같이, 사용자의 ID(리프 ID), 소유권 플래그, 사용 개시 시각, 및 복사 횟수 등이 기술된다.

또한, 마크에는 리프 ID, 소유권 플래그, 사용 개시 시각, 및 복사 횟수 등의 메시지에 기초하여 생성된 디지털 서명이 부가된다.

소유권 플래그는 예를 들면, 소정의 기간만큼 콘텐츠를 사용 가능하게 하는 라이센스를, 그대로 매입하도록 한 경우(사용 기간을 영구히 변경하도록 한 경우)에 부가된다. 사용 개시 시각은 콘텐츠의 사용을 소정의 기간 내에 개시한 경우에 기술된다. 예를 들면, 콘텐츠를 다운로드하는 시기가 제한되어 있는 경우에 있어서, 그 기한 내에 다운로드가 행하여졌을 때, 그 실제로 콘텐츠를 다운로드한 일시가 여기에 기술된다. 이에 의해, 기간 내에서의 유효한 사용이라는 것이 증명된다.

복사 횟수에는 지금까지 그 콘텐츠를 복사한 횟수가 이력(로그)으로서 기술된다.

다음에, 도 33의 흐름도를 참조하여, 사용자가 라이센스를 산 경우에, 마크를 부가하는 처리에 대하여 마크를 콘텐츠에 부가하는 예로서 설명한다.

처음에, 단계 S221에 있어서, CPU(21)는 입력부(26)로부터의 사용자 지령에 기초하여 인터넷(2)을 통해 라이센스 서버(4)에 액세스한다.

단계 S222에 있어서, CPU(21)는 사용자로부터의 입력부(26)를 통한 입력을 저장하고, 그 입력에 대응하여 라이센스 서버(4)에 대하여 라이센스의 매입을 요구한다.

이 요구에 대응하여, 도 34의 흐름도를 참조하여 후술하는 바와 같이, 라이센스 서버(4)는 라이센스를 매입하기 위해서 필요한 대가를 제시해 온다(도 34의 단계 S242). 따라서, 단계 S223에 있어서, 클라이언트(1)의 CPU(21)는 라이센스 서버(4)로부터의 대가 제시를 수취하면, 이것을 출력부(27)에 출력하여 표시시킨다.

사용자는 이 표시에 기초하여, 제시된 대가를 승낙할지의 여부를 판단하고, 그 판단 결과에 기초하여 입력부(26)로부터 그 판단 결과를 입력한다.

CPU(21)는 단계 S224에 있어서, 입력부(26)로부터의 입력에 기초하여, 사용자가 제시된 대가를 승낙할지의 여부를 판정하고, 승낙하였다고 판정한 경우에는, 단계 S225로 진행하여, 라이센스 서버(4)에 승낙을 통지하는 처리를 실행한다.

이 승낙 통지를 수신하면, 라이센스 서버(4)는 대가의 매입을 나타내는 정보, 즉 소유권 플래그를 기술한 마크를 송신해 온다(도 34의 단계 S244). 따라서, 단계 S226에 있어서, 클라이언트(1)의 CPU(21)는, 라이센스 서버(4)로부터의 마크를 수취하면, 단계 S227에 있어서, 수취한 마크를 콘텐츠에 매립하는 처리를 실행한다. 즉, 이에 의해, 매입된 라이센스에 대응하는 콘텐츠의 마크로서, 도 32에 도시한 바와 같은 소유권 플래그가 기술된 마크가 콘텐츠에 대응하여 기록되게 된다. 또한, 이 때, CPU(21)는 메시지가 갱신되게 되므로, 디지털 서명(도 26)도 갱신하여 기록 매체에 기록

한다.

단계 S224에 있어서, 라이센스 서버(4)로부터 제시된 대가가 승낙되지 않았다고 판정된 경우, 단계 S228로 진행하여, CPU(21)는 제시된 대가를 승낙하지 않는다는 것을 라이센스 서버(4)에 통지한다.

이러한 클라이언트(1)의 처리에 대응하여, 라이센스 서버(4)는 도 34의 흐름도에 도시한 처리를 실행한다.

즉, 처음에, 단계 S241에 있어서, 라이센스 서버(4)의 CPU(21)는, 클라이언트(1)로부터 라이센스 매입의 요구가 송신되어 오면(도 33의 단계 S222), 이것을 수취하고, 단계 S242에 있어서, 대상으로 되어 있는 라이센스의 매입에 필요한 대가를 기억부(28)로부터 판독하고, 이것을 클라이언트(1)에 송신한다.

상술한 바와 같이, 이와 같이 해서 제시된 대가에 대하여, 클라이언트(1)로부터 제시된 대가를 승낙할지의 여부의 통지가 송신되어 온다.

따라서, 단계 S243에 있어서, 라이센스 서버(4)의 CPU(21)는 클라이언트(1)로부터 승낙 통지를 수신하였는지의 여부를 판정하고, 승낙 통지를 수신하였다고 판정한 경우, 단계 S244로 진행하여, 대상이 되는 라이센스의 매입을 나타내는 메시지를 포함하는 마크를 생성하고, 자기 자신의 비밀 키로 디지털 서명을 부가하여 클라이언트(1)에 송신한다. 이와 같이 하여 송신된 마크는 상술한 바와 같이, 클라이언트(1)의 기억부(28)에서, 대응하는 콘텐츠에 기록된다(도 33의 단계 S227).

단계 S243에 있어서, 클라이언트(1)로부터 승낙 통지가 수신되지 않았다고 판정된 경우, 단계 S244의 처리는 스킵된다. 즉, 이 경우에는 라이센스의 매입 처리가 최종적으로 행해지지 않은 것으로 되기 때문에, 마크는 송신되지 않는다.

도 35는 단계 S244에 있어서, 라이센스 서버(4)로부터 클라이언트(1)에 대하여 송신되는 마크의 구성예를 도시하고 있다. 이 예에서는 그 사용자의 리프 ID, 소유권 플래그(Own), 및 리프 ID와 소유권 플래그를 라이센스 서버(4)의 비밀 키 S에 기초하여 생성된 디지털 서명 Sigs(LeafID, Own)에 의해 마크가 구성되어 있다.

또, 이 마크는 특정한 사용자의 특정한 콘텐츠에 대해서만 유효한 것이기 때문에, 대상이 되는 콘텐츠가 복사된 경우에는, 그 복사된 콘텐츠에 부수하는 마크는 무효가 된다.

이와 같이 하여, 콘텐츠와 라이센스를 분리하고, 사용 조건을 라이센스에 대응시키는 경우에도, 개개의 콘텐츠의 사용 상황에 따른 서비스를 실현하는 것이 가능해진다.

다음에, 그룹화에 대하여 설명한다. 복수의 기기나 미디어를 적당하게 모으고, 그 하나의 집합 내에서는 콘텐츠를 자유롭게 수수할 수 있도록 하는 것은 그룹화라 불린다. 통상적으로 이 그룹화는 개인이 소유하는 기기나 미디어에서 행해진다. 이 그룹화는 종래 그룹마다 그룹 키를 설정하는 등으로 하여 행해지고 있었지만, 그룹화하는 복수의 기기나 미디어에 동일한 라이센스를 대응시키는 것에 의해, 용이하게 그룹화하는 것이 가능해진다.

또한, 각 기기를 미리 등록해 둠으로써 그룹화하는 것도 가능하다. 이 경우의 그룹화에 대하여 이하에 설명한다.

이 경우, 사용자는 그룹화 대상이 되는 기기의 증명서를 미리 서버에 등록해 놓을 필요가 있다. 이 증명서의 등록 처리에 대하여 도 36과 도 37의 흐름도를 참조하여 설명한다.

처음에, 도 36의 흐름도를 참조하여, 클라이언트(그룹화 대상이 되는 기기)의 증명서의 등록 처리에 대하여 설명한다. 단계 S261에서, 클라이언트(1)의 CPU(21)는 그룹화의 대상이 되는 기기로서의 자기 자신의 증명서를 작성한다. 이 증명서에는 자기 자신의 공개 키가 포함된다.

다음에, 단계 S262로 진행하여, CPU(21)는 사용자의 입력부(26)로부터의 입력에 기초하여 콘텐츠 서버(3)를 액세스하고, 단계 S263에 있어서, 단계 S261의 처리에서 작성된 증명서를 콘텐츠 서버(3)에 송신하는 처리를 실행한다.

또, 증명서로서는 라이센스 서버(4)로부터 수신한 것을 그대로 사용할 수도 있다.

이상의 처리는 그룹화 대상이 되는 모든 기기가 행한다.

다음에, 도 37의 흐름도를 참조하여, 도 36의 클라이언트(1)의 증명서의 등록 처리에 대응하여 행해지는 콘텐츠 서버(3)의 증명서의 등록 처리에 대하여 설명한다.

처음에, 단계 S271에 있어서, 콘텐츠 서버(3)의 CPU(21)는 클라이언트(1)로부터 송신되어 온 증명서를 수신하면, 단계 S272에서 그 증명서를 기억부(28)에 등록한다.

이상의 처리가 그룹 대상이 되는 기기마다 행해진다. 그 결과, 콘텐츠 서버(3)의 기억부(28)에는 예를 들면, 도 38에 도시한 바와 같이, 그룹마다 그 그룹을 구성하는 디바이스의 증명서가 등록된다.

도 38에 도시한 예에서는, 그룹 1의 증명서로서 증명서 C11 내지 C14가 등록되어 있다. 이들 증명서 C11 내지 C14에는 대응하는 공개 키 K_{p11} 내지 K_{p14} 가 포함되어 있다.

마찬가지로, 그룹 2의 증명서로서 증명서 C21 내지 C23이 등록되어 있고, 이들은 대응하는 공개 키 K_{p21} 내지 K_{p23} 이 포함되어 있다.

이상과 같은 그룹을 구성하는 각 기기마다 그 증명서가 등록된 상태에서, 사용자로부터 그 그룹에 속하는 기기에 콘텐츠의 제공이 요구되면, 콘텐츠 서버(3)는 도 39의 흐름도에 도시한 처리를 실행한다.

처음에, 단계 S281에 있어서, 콘텐츠 서버(3)의 CPU(21)는 기억부(28)에 기억되어 있는 증명서 중, 그 그룹에 속하는 증명서를 검증하는 처리를 실행한다.

이 검증 처리는 도 30과 도 31을 참조하여 설명한 바와 같이, 각 기기의 증명서에 포함되는 리프 ID에 기초하여, 태그를 이용하여 EKB를 찾아감으로써 행해진다. EKB는 콘텐츠 서버(3)에도 라이센스 서버(4)로부터 배포되어 있다. 이 검증 처리에 의해, 리보크되어 있는 증명서는 제외된다.

단계 S282에 있어서, 콘텐츠 서버(3)의 CPU(21)는 단계 S281의 검증 처리 결과, 유효로 된 증명서를 선택한다. 그리고, 단계 S283에 있어서, CPU(21)는 단계 S282의 처리에서 선택된 각 기기의 증명서의 각 공개 키로 콘텐츠 키를 암호화한다. 단계 S284에 있어서, CPU(21)는 대상이 되는 그룹의 각 기기에, 단계 S283의 처리에서 암호화된 콘텐츠 키를 콘텐츠와 함께 송신한다.

도 38에 도시한 그룹 1 중 예를 들면 증명서 C14가 리보크되어 있다고 하면, 단계 S283의 처리에서, 예를 들면 도 40에 도시한 바와 것 같은 암호화 데이터가 생성된다.

즉, 도 40의 예에서는, 콘텐츠 키 Kc가, 증명서 C11의 공개 키 K_{p11} , 증명서 C12의 공개 키 K_{p12} , 또는 증명서 C13의 공개 키 K_{p13} 에 의해 암호화되어 있다.

콘텐츠 서버(3)의 도 39에 도시한 바와 같은 처리에 대응하여, 콘텐츠의 제공을 받는 각 그룹의 기기(클라이언트)는, 도 41의 흐름도에 도시한 처리를 실행한다.

처음에, 단계 S291에 있어서, 클라이언트(1)의 CPU(21)는, 콘텐츠 서버(3)가 도 39의 단계 S284의 처리에서 송신해 온 콘텐츠를 콘텐츠 키와 함께 수신한다. 콘텐츠는 콘텐츠 키 Kc에 의해 암호화되어 있고, 콘텐츠 키는 상술한 바와 같이 각 기기가 보유하는 공개 키에 의해 암호화되어 있다(도 40).

따라서, 단계 S292에 있어서, CPU(21)는 단계 S291의 처리에서 수신한 자신 앞의 콘텐츠 키를 자기 자신의 비밀 키로 복호하여 취득한다. 그리고, 취득한 콘텐츠 키를 이용하여 콘텐츠의 복호 처리가 행해진다.

예를 들면, 도 40의 예에 도시한 증명서 C11에 대응하는 기기는, 공개 키 K_{p11} 에 대응하는 자기 자신의 비밀 키를 이용하여 콘텐츠 키 Kc의 암호를 복호하고, 콘텐츠 키 Kc를 취득한다. 그리고, 콘텐츠 키 Kc를 이용하여 콘텐츠가 더 복호된다.

마찬가지의 처리는, 증명서 C12, C13에 대응하는 기기에서도 행해진다. 리보크되어 있는 증명서 C14의 기기는, 자기 자신의 공개 키를 이용하여 암호화된 콘텐츠 키 Kc가 콘텐츠에 부수하여 전송되어 오지 않기 때문에, 콘텐츠 키 Kc를 복호할 수 없으며, 따라서, 콘텐츠 키 Kc를 이용하여 콘텐츠를 복호할 수 없다.

이상에서는 콘텐츠 키(즉 콘텐츠)에 대하여 그룹화를 행하도록 하였지만, 라이센스 키(라이센스)에 대하여 그룹화를 행하는 것도 가능하다.

이상과 같이 하여, 특별한 그룹 키나 후술하는 ICV(Integrity Check Value)를 이용하지 않고서 그룹화가 가능해진다. 이 그룹화는 소규모의 그룹에 적용하는 데에 적합하다.

본 발명에서는, 라이센스도 체크아웃 혹은 체크인하거나, 이동하거나 복사하는 등이 가능하게 된다. 단, 이들 처리는 SDMI에서 정해진 룰에 기초하여 행해진다.

다음에, 도 42와 도 43의 흐름도를 참조하여, 이러한 클라이언트에 의한 라이센스의 체크아웃 처리에 대하여 설명한다.

처음에, 도 42의 흐름도를 참조하여 다른 클라이언트에 라이센스를 체크아웃하는 클라이언트의 처리에 대하여 설명한다. 처음에, 단계 S301에 있어서, 클라이언트(1)의 CPU(21)는 체크아웃 대상의 라이센스의 체크아웃 횟수 N1을 판독한다. 이 체크아웃 횟수는 도 8에 도시한 사용 조건에 기입되어 있으므로, 이 사용 조건으로부터 판독된다.

다음에, 단계 S302에 있어서, CPU(21)는, 체크아웃 대상 라이센스의 최대 체크아웃 횟수 N2를 역시 라이센스의 사용 조건으로부터 판독한다.

그리고, 단계 S303에 있어서, CPU(21)는 단계 S301의 처리에서 판독된 체크아웃 횟수 N1과, 단계 S302의 처리에서 판독된 최대 체크아웃 횟수 N2를 비교하여, 체크아웃 횟수 N1이 최대 체크아웃 횟수 N2 보다 작은지의 여부를 판정한다.

체크아웃 횟수 N1이 최대 체크아웃 횟수 N2 보다 작다고 판정된 경우, 단계 S304로 진행하여, CPU(21)는 상대측 장치(체크아웃처의 클라이언트)의 리프 키를 상대 개개의 장치로부터 취득하고, 그 리프 키를 지금 체크아웃 대상이 되어 있는 라이센스 ID에 대응하여 기억부(28)의 체크아웃 리스트에 기억시킨다.

다음에, 단계 S305에 있어서, CPU(21)는 단계 S301의 처리에서 판독된 라이센스의 체크아웃 횟수 N1의 값을 1만큼 인크리먼트한다. 단계 S306에 있어서, CPU(21)는 라이센스의 메시지에 기초하여 ICV를 연산한다. 이 ICV에 대해서는 도 47 내지 도 51을 참조하여 후술한다. ICV를 이용하여 라이센스의 개찬을 방지하는 것이 가능해진다.

다음에, 단계 S307에 있어서, CPU(21)는 체크아웃 대상의 라이센스와, 단계 S306의 처리에서 연산된 ICV를, 자기 자신의 공개 키를 이용하여 암호화하고, EKB 및 증명서와 함께, 상대측 장치에 출력하여 복사시킨다. 또한, 단계 S308에 있어서, CPU(21)는 단계 S306의 처리에서 연산된 ICV를, 상대측 장치의 리프 키와 라이센스 ID에 대응하여 기억부(28)의 체크 리스트 내에 기억시킨다.

단계 S303에 있어서, 체크아웃 횟수 N1이 최대 체크아웃 횟수 N2보다 작지 않다(예를 들면, 같다)고 판정된 경우, 이미 허용받은 횟수만큼 체크아웃이 행해져 있으므로, 더 이상 체크아웃을 행할 수 없다. 따라서, 단계 S309로 진행하여, CPU(21)는 에러 처리를 실행한다. 즉, 이 경우, 체크아웃 처리는 실행되지 않게 된다.

다음에, 도 43의 흐름도를 참조하여, 도 42의 체크아웃 처리에 의해 라이센스의 체크아웃을 받는 클라이언트의 처리에 대하여 설명한다.

처음에, 단계 S321에 있어서, 상대측 장치(라이센스를 체크아웃하는 클라이언트(1))에 자기 자신의 리프 키를 송신한다. 이 리프 키는 단계 S304에 있어서, 상대측의 클라이언트에 의해 라이센스 ID에 대응하여 기억된다.

다음에, 단계 S322에 있어서, CPU(21)는 상대측의 클라이언트(1)로부터 암호화된 라이센스와 ICV가 EKB 및 증명서와 함께 송신되어 온 경우, 이것을 수신한다. 즉, 이 라이센스, ICV, EKB 및 증명서는 도 42의 단계 S307의 처리에서 상대측 장치로부터 송신된 것이다.

단계 S323에 있어서, CPU(21)는 단계 S322의 처리에서 수신한 라이센스, ICV, EKB 및 증명서를 기억부(28)에 기억시킨다.

이상과 같이 하여, 라이센스의 체크아웃을 받은 클라이언트(1)는, 체크아웃을 받은 그 라이센스를 사용하여 소정의 콘텐츠를 재생하는 경우, 도 44의 흐름도에 도시한 처리를 실행한다.

즉, 처음에, 단계 S341에 있어서, 클라이언트(1)의 CPU(21)는 사용자로부터 입력부(26)를 통해 재생이 지정된 콘텐츠의 ICV를 연산한다. 그리고, 단계 S342에 있어서, CPU(21)는 기억부(28)에 기억되어 있는 암호화되어 있는 ICV를, 증명서에 포함되어 있는 공개 키에 기초하여 복호시킨다.

다음에, 단계 S343에 있어서, CPU(21)는 단계 S341의 처리에 의해, 지금 연산된 ICV와, 단계 S342의 처리에 의해 판독되고 복호된 ICV가 일치하는지의 여부를 판정한다. 양자가 일치하는 경우에는, 라이센스는 개찬되어 있지 않게 된다. 따라서, 단계 S344로 진행하여, CPU(21)는 대응하는 콘텐츠를 재생하는 처리를 실행한다.

이에 대하여, 단계 S343에 있어서, 2개의 ICV가 일치하지 않는다고 판정된 경우, 라이센스는 개찬되어 있을 우려가 있다. 이 때문에, 단계 S345로 진행하여, CPU(21)는 에러 처리를 실행한다. 즉, 이 때, 그 라이센스를 이용하여 콘텐츠를 재생할 수 없게 된다.

다음에, 이상과 같이 하여, 다른 클라이언트에 일단 체크아웃한 라이센스의 체크인을 받는 클라이언트의 처리에 대하여, 도 45의 흐름도를 참조하여 설명한다.

처음에, 단계 S361에 있어서, CPU(21)는 상대측 장치(라이센스를 반환(체크인)하여 오는 클라이언트(1))의 리프 키와, 체크인 대상의 라이센스 ID를 취득한다. 다음에, 단계 S3162에 있어서, CPU(21)는 단계 S361에서 취득된 체크인 대상의 라이센스가, 자기 자신이 상대측 장치에 체크아웃한 라이센스인지의 여부를 판정한다. 이 판정은 도 42의 단계 S308의 처리에서 기억된 ICV, 리프 키, 및 라이센스 ID에 기초하여 행해진다. 즉, 단계 S361에서 취득된 리프 키, 라이센스 ID, 및 ICV가 체크아웃 리스트 중에 기억되어 있는지의 여부가 판정되고, 기억되어 있는 경우에는, 자기 자신이 체크아웃한 라이센스라고 판정된다.

라이센스가 자기 자신이 체크아웃한 것일 때, 단계 S363에 있어서, CPU(21)는 상대측 장치의 라이센스, EKB 및 증명서의 삭제를 요구한다. 후술하는 바와 같이, 이 요구에 기초하여, 상대측 장치는 라이센스, EKB 및 증명서의 삭제를 실행한다(도 46의 단계 S383).

단계 S364에 있어서, CPU(21)는 일단 체크아웃한 라이센스가 다시 체크인되었기 때문에, 그 라이센스의 체크아웃 횟수 N1을 1만큼 디크리먼트한다.

단계 S365에 있어서, CPU(21)는 상대측 장치에 다른 라이센스를 체크아웃하고 있는지의 여부를 판정하고, 아직 체크아웃하고 있는 다른 라이센스가 존재하지 않은 경우에는, 단계 S366으로 진행하여, CPU(21)는 상대측 장치의 체크인

대상 기기로서의 체크아웃 리스트에서의 기억을 삭제한다. 이에 대하여, 단계 S365에 있어서, 상대측 장치에 체크아웃하고 있는 다른 라이센스가 존재한다고 판정된 경우에는, 다른 라이센스의 체크인을 받을 가능성이 있으므로, 단계 S366의 처리는 스킵된다.

단계 S362에 있어서, 체크인 대상이 되어 있는 라이센스가 자기 자신이 상대측 장치에 체크아웃한 라이센스가 아니라고 판정된 경우, CPU(21)는 단계 S367로 진행하여 에러 처리를 실행한다. 즉, 이 경우에는 자기 자신이 관할하는 라이센스가 아니게 되므로, 체크인 처리는 실행되지 않는다.

사용자가 라이센스를 부정하게 복사한 등의 경우, 기억되어 있는 ICV의 값과, 단계 S361의 처리에서 취득된 라이센스에 기초하여 연산된 ICV의 값이 다르게 되므로, 체크인할 수 없게 된다.

도 46은 도 45의 흐름도에 도시한 라이센스의 체크인 처리를 실행하는 클라이언트에 대하여, 자기 자신이 갖고 있는 라이센스를 체크인시키는 클라이언트의 처리를 도시하고 있다.

단계 S381에 있어서, 클라이언트(1)의 CPU(21)는, 상대측 장치(도 45의 흐름도에 도시한 처리를 실행하는 클라이언트(1))에 리프 키와 체크인 대상의 라이센스의 ID를 송신한다. 상술한 바와 같이, 상대측 장치는 단계 S361에 있어서, 이 리프 키와 라이센스 ID를 취득하고, 단계 S362에 있어서, 그것에 기초하여 체크인 대상의 라이센스 인증 처리를 실행한다.

단계 S382에 있어서, 클라이언트(1)의 CPU(21)는 상대측 장치로부터 라이센스 삭제를 요구받았는지의 여부를 판정한다. 즉, 라이센스가 정당한 체크인 대상의 라이센스인 경우, 상술한 바와 같이, 상대측 장치는 단계 S363의 처리에서 라이센스, EKB 및 증명서의 삭제를 요구해 온다. 따라서, 이 요구를 수신한 경우, 단계 S383으로 진행하여, CPU(21)는 라이센스, EKB 및 증명서를 삭제한다. 즉, 이에 의해, 이 클라이언트(1)는 이 후에 그 라이센스를 사용할 수 없는 상태로 되고, 도 45의 단계 S364의 처리에 의해, 체크아웃 횟수 N1이 1만큼 디크리먼트되기 때문에, 체크인이 완료되게 된다.

단계 S382에 있어서, 상대측 장치로부터 라이센스의 삭제가 요구되지 않았다고 판정된 경우, 단계 S384로 진행하여, 에러 처리가 실행된다. 즉, 이 경우에는 ICV의 값이 다르다는 등의 이유에 의해 체크인을 할 수 없게 된다.

이상에서는 체크인과 체크아웃에 대하여 설명하였지만, 마찬가지로 라이센스를 복사 혹은 이동시키도록 하는 것도 가능하다.

다음에, 라이센스(콘텐츠도 마찬가지)의 개찬을 방지하기 위해서 라이센스의 인티그리티 체크값(ICV)을 생성하고, 라이센스에 대응하여, ICV의 계산에 의해 라이센스 개찬의 유무를 판정하는 처리 구성에 대하여 설명한다.

라이센스의 인티그리티 체크값(ICV)은, 예를 들면 라이센스에 대한 해시 함수를 이용하여 계산되고, ICV=hash(Kicv, L1, L2, …)에 의해 계산된다. Kicv는 ICV 생성 키이다. L1, L2는 라이센스의 정보이며, 라이센스의 중요 정보의 메시지 인증 부호(MAC: Message Authentication Code)가 사용된다.

DES 암호 처리 구성을 이용한 MAC값 생성 예를 도 47에 도시한다. 도 47의 구성에 도시한 바와 같이 대상이 되는 메시지를 8바이트 단위로 분할하고, (이하, 분할된 메시지를 M1, M2, …, MN으로 함), 먼저, 초기값(IV)과 M1을, 연산부(24-1A)에 의해 배타적 논리합한다(그 결과를 I1로 함). 다음에, I1을 DES 암호화부(24-1B)에 넣고, 키(이하, K1로 함)를 이용하여 암호화한다(출력을 E1로 함). 계속하여, E1 및 M2를 연산부(24-2A)에 의해 배타적 논리합하고, 그 출력 I2를 DES 암호화부(24-2B)에 넣고, 키 K1을 이용하여 암호화한다(출력 E2). 이하, 이것을 반복하여, 모든 메시지에 대하여 암호화 처리를 실시한다. DES 암호화부(24-NB)에서 마지막으로 나온 EN이 메시지 인증 부호(MAC(Message Authentication Code))가 된다.

이러한 라이센스의 MAC값과 ICV 생성 키에 해시 함수를 적용하여 라이센스의 인티그리티 체크값(ICV)이 생성된다. 예를 들면 라이센스 생성 시에 생성한 ICV와, 새롭게 라이센스에 기초하여 생성한 ICV를 비교하여 동일한 ICV가 얻어지면 라이센스에 개찬이 없다는 것이 보증되고, ICV가 다르면 개찬이 있었다고 판정된다.

다음에, 라이센스의 인티그리티 체크값(ICV) 생성 키인 Kicv를 상술한 유효화 키 블록에 의해서 송부하는 구성에 대하여 설명한다. 즉 EKB에 의한 암호화 메시지 데이터를 라이센스의 인티그리티 체크값(ICV) 생성 키로 한 예이다.

도 48 및 도 49에 복수의 디바이스에 공통의 라이센스를 송부한 경우, 이들 라이센스의 개찬 유무를 검증하기 위한 인티그리티 체크값 생성 키 Kicv를 유효화 키 블록(EKB)에 의해서 배신하는 구성예를 도시한다. 도 48은 디바이스 0, 1, 2, 3에 대하여 복호 가능한 체크값 생성 키 Kicv를 배신하는 예를 도시하고, 도 49는 디바이스 0, 1, 2, 3 중의 디바이스 3을 리보크(배제)하여 디바이스 0, 1, 2에 대해서만 복호 가능한 체크값 생성 키 Kicv를 배신하는 예를 도시한다.

도 48의 예에서는, 갱신 노드 키 K(t)00에 의해서, 체크값 생성 키 Kicv를 암호화한 데이터 Enc(K(t)00, Kicv)와 함께, 디바이스 0, 1, 2, 3에서 각각이 갖는 노드 키, 리프 키를 이용하여 갱신된 노드 키 K(t)00을 복호 가능한 유효화 키 블록(EKB)을 생성하여 배신한다. 각각의 디바이스는 도 48의 우측에 도시한 바와 같이, 먼저 EKB를 처리(복호)함으로써, 갱신된 노드 키 K(t)00을 취득하고, 다음에, 취득한 노드 키 K(t)00을 이용하여, 암호화된 체크값 생성 키 Enc(K(t)00, Kicv)를 복호하여, 체크값 생성 키 Kicv를 얻는 것이 가능해진다.

그 밖의 디바이스 4, 5, 6, 7…은 동일한 유효화 키 블록(EKB)을 수신해도 자신이 보유하는 노드 키, 리프 키에서는 EKB를 처리하여 갱신된 노드 키 K(t)00을 취득할 수 없기 때문에, 안전하게 정당한 디바이스에 대해서만 체크값 생성 키를 송부할 수 있다.

한편, 도 49의 예는 도 12의 점선으로 표시된 그룹에서 디바이스 3이, 예를 들면 키의 누설에 의해 리보크(배제)되어 있다고 하고, 다른 그룹의 멤버, 즉 디바이스 0, 1, 2에 대해서만 복호 가능한 유효화 키 블록(EKB)을 생성하여 배신한 예이다. 도 49에 도시한 유효화 키 블록(EKB)과, 체크값 생성 키(Kicv)를 노드 키(K(t)00)로 암호화한 데이터 Enc(K(t)00, Kicv)를 배신한다.

도 49의 우측에는 복호 수순이 도시되어 있다. 디바이스 0, 1, 2는 먼저, 수령한 유효화 키 블록으로부터 자신이 보유하는 리프 키 또는 노드 키를 이용한 복호 처리에 의해, 갱신 노드 키(K(t)00)를 취득한다. 다음에, K(t)00에 의한 복호에 의해 체크값 생성 키 Kicv를 취득한다.

도 12에 도시한 다른 그룹의 디바이스 4, 5, 6…은 이와 마찬가지 데이터(EKB)를 수신하였다고 해도, 자신이 보유하는 리프 키, 노드 키를 이용하여 갱신 노드 키(K(t)00)를 취득할 수 없다. 마찬가지로 리보크된 디바이스 3에 있어서도, 자신이 보유하는 리프 키, 노드 키에서는 갱신 노드 키(K(t)00)를 취득할 수 없으며, 정당한 권리를 갖는 디바이스만이 체크값 생성 키를 복호하여 이용하는 것이 가능해진다.

이와 같이, EKB를 이용한 체크값 생성 키의 배송을 이용하면, 데이터 량을 적게 하면서도 안전하게 정당 권리자만이 복호 가능하게 한 체크값 생성 키를 배신하는 것이 가능해진다.

이러한 라이센스의 인티그리티 체크값(ICV)을 이용함으로써, EKB와 암호화 라이센스의 부정 복사를 배제할 수 있다. 예를 들면 도 50A에 도시한 바와 같이, 라이센스 L1과 라이센스 L2를 각각의 라이센스 키를 취득 가능한 유효화 키 블록(EKB)과 함께 저장한 미디어 1이 있고, 이것을 그대로 미디어 2에 복사한 경우를 상정한다. EKB와 암호화 라이센스의 복사는 가능하고, 이것을, EKB를 복호할 수 있는 디바이스에서는 이용할 수 있게 된다.

도 50B에 도시한 예에서는 각 미디어에 정당하게 저장된 라이센스에 대응하여 인티그리티 체크값(ICV(L_1, L_2))을 저장하는 구성으로 한다. 또, (ICV(L_1, L_2))는 라이센스 L1과 라이센스 L2에 해시 함수를 이용하여 계산되는 라이센스의 인티그리티 체크값인 ICV=hash(Kicv, L_1, L_2)를 도시하고 있다. 도 50B의 구성에 있어서, 미디어 1에는 정당하게 라이센스 1과 라이센스 2가 저장되고, 라이센스 L1과 라이센스 L2에 기초하여 생성된 인티그리티 체크값(ICV(L_1, L_2))이 저장된다. 또한, 미디어 2에는 정당하게 라이센스 1이 저장되고, 라이센스 L1에 기초하여 생성된 인티그리티 체크값(ICV(L_1))이 저장된다.

이 구성에 있어서, 미디어 1에 저장된 {EKB, 라이센스 2}를 미디어 2에 복사하였다고 하면, 미디어 2에서, 라이센스 체크값을 새롭게 생성하면, ICV(L_1, L_2)가 생성되게 되고, 미디어 2에 저장되어 있는 Kicv(L1)와 달리, 라이센스의 개찬 혹은 부정한 복사에 의한 새로운 라이센스의 저장이 실행되었음이 명백해진다. 미디어를 재생하는 디바이스에 있어서, 재생 단계 이전 단계에 ICV 체크를 실행하고, 생성 ICV와 저장 ICV의 일치를 판별하여, 일치하지 않은 경우에는, 재생을 실행하지 않은 구성으로 함으로써, 부정 복사의 라이센스 재생을 방지하는 것이 가능해진다.

그리고 또한, 안전성을 높이기 위해서, 라이센스의 인티그리티 체크값(ICV)을 재기입하여 카운터를 포함시킨 데이터에 기초하여 생성하는 구성으로 하여도 된다. 즉 ICV=hash(Kicv, counter+1, L1, L2, …)에 의해 계산하는 구성으로 한다. 여기서, 카운터(counter+1)는 ICV의 재기입마다 1 인크리먼트되는 값으로서 설정한다. 또, 카운터값은 시큐어한 메모리에 저장하는 구성으로 하는 것이 필요하다.

또한, 라이센스의 인티그리티 체크값(ICV)을 라이센스와 동일 미디어에 저장할 수 없는 구성에 있어서는, 라이센스의 인티그리티 체크값(ICV)을 라이센스와는 별도의 미디어 상에 저장하는 구성으로 하여도 된다.

예를 들면, 판독 전용 미디어나 통상의 MO 등의 복사 방지책이 취해져 있지 않은 미디어에 라이센스를 저장하는 경우, 동일 미디어에 인티그리티 체크값(ICV)을 저장하면 ICV의 재기입이 부정한 사용자에 의해 이루어질 가능성이 있으며, ICV의 안전성을 유지할 수 없을 우려가 있다. 이와 같은 경우, 호스트 머신 상의 안전한 미디어에 ICV를 저장하고, 라이센스의 복사 컨트롤(예를 들면 check-in/check-out, move)에 ICV를 사용하는 구성으로 함으로써, ICV의 안전한 관리 및 라이센스의 개찬 체크가 가능해진다.

이 구성 예를 도 51에 도시한다. 도 51에서는 판독 전용 미디어나 통상의 MO 등의 복사 방지책이 취해져 있지 않은 미디어(2201)에 라이센스 1 내지 라이센스 3이 저장되고, 이들 라이센스에 관한 인티그리티 체크값(ICV)을, 사용자가 자유롭게 액세스하는 것이 허가되지 않은 호스트 머신 상의 안전한 미디어(2202)에 저장하여, 사용자에 의한 부정한 인티그리티 체크값(ICV)의 재기입을 방지한 예이다. 이러한 구성으로 하여, 예를 들면 미디어(2201)를 장착한 디바이스가, 미디어(2201)의 재생을 실행할 때에 호스트 머신인 PC, 서버에 있어서 ICV의 체크를 실행하여 재생 가부를 판정하는 구성으로 하면, 부정한 복사 라이센스 혹은 개찬 라이센스의 재생을 방지할 수 있다.

본 발명이 적용되는 클라이언트는 소위 퍼스널 컴퓨터 이외에, PDA(Personal Digital Assistants), 휴대 전화기, 게임 단말기 등으로 할 수 있다.

일련의 처리를 소프트웨어에 의해 실행시키는 경우에는, 그 소프트웨어를 구성하는 프로그램이, 전용의 하드웨어에 조립되어 있는 컴퓨터, 또는 각종 프로그램을 인스톨함으로써, 각종 기능을 실행하는 것이 가능한, 예를 들면 범용의 퍼스널 컴퓨터 등에 네트워크나 기록 매체로부터 인스톨된다.

이 기록 매체는 도 2에 도시한 바와 같이, 장치 본체와는 별도로, 사용자에게 프로그램을 제공하기 위해서 배포되는, 프로그램이 기록되어 있는 자기 디스크(41)(플로피 디스크를 포함함), 광 디스크(42)(CD-ROM(Compact Disk-Read Only Memory), DVD(Digital Versatile Disk)를 포함함), 광 자기 디스크(43)(MD(Mini-Disk)를 포함함), 혹은 반도체 메모리(44) 등으로 이루어지는 패키지 미디어로 구성되는 것 뿐만 아니라, 장치 본체에 사전에 내장된 상태에

서 사용자에게 제공되는, 프로그램이 기록되어 있는 ROM(22)이나, 기억부(28)에 포함되는 하드디스크 등으로 구성된다.

또, 본 명세서에 있어서, 기록 매체에 기록되는 프로그램을 기술하는 단계는, 기재된 순서에 따라서 시계열적으로 행해지는 처리는 물론, 반드시 시계열적으로 처리되지 않더라도, 병렬적 혹은 개별로 실행되는 처리도 포함하는 것이다.

또한, 시큐러티에 관련된 처리를 실행시키는 프로그램은, 그 처리가 해석되는 것을 방지하기 위해서, 그 프로그램 자체가 암호화되어 있는 것이 바람직하다. 예를 들면, 암호 처리 등을 행하는 처리에 대해서는 그 프로그램을 탬퍼 레지스턴트 모듈로서 구성할 수 있다.

또한, 콘텐츠를 이용 허가하는 라이센스를 특정하기 위해서 콘텐츠의 헤더에 기재되어 있는 정보는 라이센스를 일의적으로 식별하는 라이센스 ID가 아니더라도 무방하다. 상기 실시예에서는, 라이센스 ID가, 콘텐츠의 이용에 필요한 라이센스를 특정하는 정보이고, 어떤 라이센스가 이용을 허가하는 콘텐츠를 특정하는 정보이며, 클라이언트(1)로부터 라이센스 요구에 따라서 요구되는 라이센스를 식별하는 정보이다. 콘텐츠에 콘텐츠의 그 콘텐츠에 관한 각종 속성 정보의 리스트가 기재되고, 라이센스에 그 라이센스에 의해서 이용 허가되는 콘텐츠의 조건식을 기재하도록 하여도 된다. 이 경우에는, 콘텐츠에 포함되는 속성 정보가 그 콘텐츠의 이용을 허가하는 라이센스를 특정하는 정보이고, 라이센스에 포함되는 조건식이 그 라이센스가 이용을 허가하는 콘텐츠를 특정하는 정보이고, 라이센스 ID는 라이센스를 일의적으로 식별하는 정보가 된다. 이와 같이 한 경우에는, 하나의 콘텐츠에 복수의 라이센스를 대응시키는 것이 가능하게 되어, 라이센스의 발행을 유연하게 행할 수 있다.

또한, 콘텐츠 데이터는 음악 데이터에 한하지 않는다. 예를 들면 콘텐츠는 화상 데이터, 동화상 데이터, 텍스트 데이터, 애니메이션 데이터, 소프트웨어 프로그램, 혹은 이들을 조합한 것이어도 된다.

또한, 본 명세서에 있어서, 시스템이란 복수의 장치로 구성되는 장치 전체를 나타내는 것이다.

산업상 이용 가능성

본 발명의 제1 정보 처리 장치에 따르면, 워터마크를 포함하는 헤더, 증명서, 디지털 서명, 암호화된 콘텐츠, 및 키 정보를 파일 포맷으로 포맷화하도록 하였으므로, 예를 들면, SDMI에서의 저작권 관리 시스템은 원래부터, 인터넷으로 대표되는 네트워크 등을 통해 전송되는 시스템에서의 콘텐츠의 저작권 관리도 가능한 포맷으로, 콘텐츠를 출력하는 것이 가능해진다.

본 발명의 제2 정보 처리 장치에 따르면, 증명서와 디지털 서명을 이용하여 검증을 행하고, 헤더의 워터마크에 기초하여, 콘텐츠의 출력을 제어하도록 하였으므로, 예를 들면, SDMI의 시스템에 위반되는 부정하게 복사된 콘텐츠의 사용이나, 예를 들면, 인터넷 등에 의해 부정하게 복사된 콘텐츠의 사용을 확실하게 제어하는 것이 가능해진다.

(57) 청구의 범위

청구항 1.

콘텐츠를 제공하는 정보 처리 장치에 있어서,

상기 콘텐츠를 취득하는 콘텐츠 취득 수단과,

상기 콘텐츠 취득 수단에 의해 취득된 상기 콘텐츠에 부가되어 있는 워터마크를 추출하는 추출 수단과,

상기 추출 수단에 의해 추출된 상기 워터마크를 포함하는 헤더를 작성하는 헤더 작성 수단과,

비밀 키를 이용하여, 상기 헤더 작성 수단에 의해 작성된 상기 헤더의 데이터에 기초한 디지털 서명을 작성하는 디지털 서명 작성 수단과,

상기 콘텐츠 취득 수단에 의해 취득된 상기 콘텐츠를 암호화하는 암호화 수단과,

상기 암호화 수단에 의해 암호화된 상기 콘텐츠를 복호하는데 필요한 키 정보를 포함하는 키 정보를 취득하는 키 정보 취득 수단과,

상기 헤더 작성 수단에 의해 작성된 상기 헤더, 상기 디지털 서명 작성 수단에 의해 작성된 상기 디지털 서명, 상기 암호화 수단에 의해 암호화된 상기 콘텐츠, 및 상기 키 정보 취득 수단에 의해 취득된 상기 키 정보를, 파일 포맷으로 포맷화하여, 출력하는 포맷화 수단

을 포함하는 것을 특징으로 하는 정보 처리 장치.

청구항 2.

제1항에 있어서,

상기 워터마크는, 복사 관리 정보를 포함하는 것을 특징으로 하는 정보 처리 장치.

청구항 3.

제1항에 있어서,

상기 헤더 작성 수단에 의해 작성된 상기 헤더는, 상기 콘텐츠를 식별하는 콘텐츠 식별 정보, 및 상기 콘텐츠의 라이센스를 특정하는 라이센스 특정 정보를 더 포함하는 것을 특징으로 하는 정보 처리 장치.

청구항 4.

제1항에 있어서,

상기 비밀 키에 대응하는 공개 키를 포함하는 증명서를 취득하는 증명서 취득 수단을 더 포함하며,

상기 포맷화 수단은, 또한, 상기 증명서 취득 수단에 의해 취득된 상기 증명서를, 상기 파일 포맷으로 포맷화하여, 출력하는 것을 특징으로 하는 정보 처리 장치.

청구항 5.

콘텐츠를 제공하는 정보 처리 장치의 정보 처리 방법에 있어서,

상기 콘텐츠를 취득하는 콘텐츠 취득 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는 워터마크를 추출하는 추출 단계와,

상기 추출 단계의 처리에 의해 추출된 상기 워터마크를 포함하는 헤더를 작성하는 헤더 작성 단계와,

비밀 키를 이용하여, 상기 헤더 작성 단계의 처리에 의해 작성된 상기 헤더의 데이터에 기초한 디지털 서명을 작성하는 디지털 서명 작성 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠를 암호화하는 암호화 단계와,

상기 암호화 단계의 처리에 의해 암호화된 상기 콘텐츠를 복호하는 데 필요한 키 정보를 포함하는 키 정보를 취득하는 키 정보 취득 단계와,

상기 헤더 작성 단계의 처리에 의해 작성된 상기 헤더, 상기 디지털 서명 작성 단계의 처리에 의해 작성된 상기 디지털 서명, 상기 암호화 단계의 처리에 의해 암호화된 상기 콘텐츠, 및 상기 키 정보 취득 단계의 처리에 의해 취득된 상기 키 정보를, 파일 포맷으로 포맷화하여, 출력하는 포맷화 단계

를 포함하는 것을 특징으로 하는 정보 처리 방법.

청구항 6.

콘텐츠를 제공하는 정보 처리 장치용의 프로그램으로서,

상기 콘텐츠를 취득하는 콘텐츠 취득 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는 워터마크를 추출하는 추출 단계와,

상기 추출 단계의 처리에 의해 추출된 상기 워터마크를 포함하는 헤더를 작성하는 헤더 작성 단계와,

비밀 키를 이용하여, 상기 헤더 작성 단계의 처리에 의해 작성된 상기 헤더의 데이터에 기초한 디지털 서명을 작성하는 디지털 서명 작성 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠를 암호화하는 암호화 단계와,

상기 암호화 단계의 처리에 의해 암호화된 상기 콘텐츠를 복호하는 데 필요한 키 정보를 포함하는 키 정보를 취득하는 키 정보 취득 단계와,

상기 헤더 작성 단계의 처리에 의해 작성된 상기 헤더, 상기 디지털 서명 작성 단계의 처리에 의해 작성된 상기 디지털 서명, 상기 암호화 단계의 처리에 의해 암호화된 상기 콘텐츠, 및 상기 키 정보 취득 단계의 처리에 의해 취득된 상기 키 정보를, 파일 포맷으로 포맷화하여, 출력하는 포맷화 단계

를 포함하는 것을 특징으로 하는 컴퓨터가 판독 가능한 프로그램이 기록되어 있는 기록 매체.

청구항 7.

콘텐츠를 제공하는 정보 처리 장치를 제어하는 컴퓨터가 실행 가능한 프로그램에 있어서,

상기 콘텐츠를 취득하는 콘텐츠 취득 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는 워터마크를 추출하는 추출 단계와,

상기 추출 단계의 처리에 의해 추출된 상기 워터마크를 포함하는 헤더를 작성하는 헤더 작성 단계와,

비밀 키를 이용하여, 상기 헤더 작성 단계의 처리에 의해 작성된 상기 헤더의 데이터에 기초한 디지털 서명을 작성하는 디지털 서명 작성 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠를 암호화하는 암호화 단계와,

상기 암호화 단계의 처리에 의해 암호화된 상기 콘텐츠를 복호하는 데 필요한 키 정보를 포함하는 키 정보를 취득하는 키 정보 취득 단계와,

상기 헤더 작성 단계의 처리에 의해 작성된 상기 헤더, 상기 디지털 서명 작성 단계의 처리에 의해 작성된 상기 디지털 서명, 상기 암호화 단계의 처리에 의해 암호화된 상기 콘텐츠, 및 상기 키 정보 취득 단계의 처리에 의해 취득된 상기 키 정보를, 파일 포맷으로 포맷화하여, 출력하는 포맷화 단계

를 포함하는 것을 특징으로 하는 프로그램.

청구항 8.

콘텐츠를 출력하는 정보 처리 장치에 있어서,

암호화되어 있는 상기 콘텐츠를 취득하는 콘텐츠 취득 수단과,

상기 콘텐츠 취득 수단에 의해 취득된 상기 콘텐츠에 부가되어 있는, 상기 콘텐츠를 복호하는 데 필요한 키 정보를 검출하는 키 정보 검출 수단과,

상기 키 정보 검출 수단에 의해 검출된 상기 키 정보를 이용하여, 상기 콘텐츠를 복호하는 데 필요한 콘텐츠 키를 취득하는 콘텐츠 키 취득 수단과,

상기 콘텐츠 키 취득 수단에 의해 취득된 상기 콘텐츠 키를 이용하여, 상기 콘텐츠 취득 수단에 의해 취득된 상기 콘텐츠를 복호하는 복호 수단과,

상기 콘텐츠 취득 수단에 의해 취득된 상기 콘텐츠에 부가되어 있는 증명서를 검출하는 증명서 검출 수단과,

상기 증명서 검출 수단에 의해 검출된 상기 증명서를, 인증국의 공개 키를 이용하여 검증하는 제1 검증 수단과,

상기 증명서 검출 수단에 의해 검출된 상기 증명서로부터, 상기 콘텐츠를 제공하는 콘텐츠 제공자의 공개 키를 취득하는 공개 키 취득 수단과,

상기 콘텐츠 취득 수단에 의해 취득된 상기 콘텐츠에 부가되어 있는, 디지털 서명을 검출하는 디지털 서명 검출 수단과,

상기 디지털 서명 검출 수단에 의해 검출된 상기 디지털 서명을, 상기 공개 키 취득 수단에 의해 취득된 상기 콘텐츠 제공자의 상기 공개 키를 이용하여 검증하는 제2 검증 수단과,

상기 콘텐츠 취득 수단에 의해 취득된 상기 콘텐츠에 부가되어 있는 헤더로부터, 워터마크를 검출하는 워터마크 검출 수단과,

상기 워터마크 검출 수단에 의해 검출된 상기 워터마크에 기초하여, 상기 콘텐츠의 출력을 제어하는 제어 수단

을 포함하는 것을 특징으로 하는 정보 처리 장치.

청구항 9.

콘텐츠를 출력하는 정보 처리 장치의 정보 처리 방법에 있어서,

암호화되어 있는 상기 콘텐츠를 취득하는 콘텐츠 취득 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는, 상기 콘텐츠를 복호하는 데 필요한 키 정보를 검출하는 키 정보 검출 단계와,

상기 키 정보 검출 단계의 처리에 의해 검출된 상기 키 정보를 이용하여, 상기 콘텐츠를 복호하는 데 필요한 콘텐츠 키를 취득하는 콘텐츠 취득 단계와,

상기 콘텐츠 키 취득 단계의 처리에 의해 취득된 상기 콘텐츠 키를 이용하여, 상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠를 복호하는 복호 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는 증명서를 검출하는 증명서 검출 단계와,

상기 증명서 검출 단계의 처리에 의해 검출된 상기 증명서를, 인증국의 공개 키를 이용하여 검증하는 제1 검증 단계와,

상기 증명서 검출 단계의 처리에 의해 검출된 상기 증명서로부터, 상기 콘텐츠 제공자의 공개 키를 취득하는 공개 키 취득 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는 디지털 서명을 검출하는 디지털 서명 검출 단계와,

상기 디지털 서명 검출 단계의 처리에 의해 검출된 상기 디지털 서명을, 상기 공개 키 취득 단계의 처리에 의해 취득된 상기 콘텐츠 제공자의 상기 공개 키를 이용하여 검증하는 제2 검증 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는 헤더로부터, 워터마크를 검출하는 워터마크 검출 단계와,

상기 워터마크 검출 단계의 처리에 의해 검출된 상기 워터마크에 기초하여, 상기 콘텐츠의 출력을 제어하는 제어 단계

를 포함하는 것을 특징으로 하는 정보 처리 방법.

청구항 10.

콘텐츠를 출력하는 정보 처리 장치용의 프로그램으로서,

암호화되어 있는 상기 콘텐츠를 취득하는 콘텐츠 취득 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는, 상기 콘텐츠를 복호하는 데 필요한 키 정보를 검출하는 키 정보 검출 단계와,

상기 키 정보 검출 단계의 처리에 의해 검출된 상기 키 정보를 이용하여, 상기 콘텐츠를 복호하는 데 필요한 콘텐츠 키를 취득하는 콘텐츠 키 취득 단계와,

상기 콘텐츠 키 취득 단계의 처리에 의해 취득된 상기 콘텐츠 키를 이용하여, 상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠를 복호하는 복호 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는 증명서를 검출하는 증명서 검출 단계와,

상기 증명서 검출 단계의 처리에 의해 검출된 상기 증명서를, 인증국의 공개 키를 이용하여 검증하는 제1 검증 단계와,

상기 증명서 검출 단계의 처리에 의해 검출된 상기 증명서로부터, 상기 콘텐츠 제공자의 공개 키를 취득하는 공개 키 취득 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는 디지털 서명을 검출하는 디지털 서명 검출 단계와,

상기 디지털 서명 검출 단계의 처리에 의해 검출된 상기 디지털 서명을, 상기 공개 키 취득 단계의 처리에 의해 취득된 상기 콘텐츠 제공자의 상기 공개 키를 이용하여 검증하는 제2 검증 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는 헤더로부터, 워터마크를 검출하는 워터마크 검출 단계와,

상기 워터마크 검출 단계의 처리에 의해 검출된 상기 워터마크에 기초하여, 상기 콘텐츠의 출력을 제어하는 제어 단계

를 포함하는 것을 특징으로 하는 컴퓨터가 판독 가능한 프로그램이 기록되어 있는 기록 매체.

청구항 11.

콘텐츠를 출력하는 정보 처리 장치를 제어하는 컴퓨터가 실행 가능한 프로그램에 있어서,

암호화되어 있는 상기 콘텐츠를 취득하는 콘텐츠 취득 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는, 상기 콘텐츠를 복호하는 데 필요한 키 정보를 검출하는 키 정보 검출 단계와,

상기 키 정보 검출 단계의 처리에 의해 검출된 상기 키 정보를 이용하여, 상기 콘텐츠를 복호하는 데 필요한 콘텐츠 키를 취득하는 콘텐츠 키 취득 단계와,

상기 콘텐츠 키 취득 단계의 처리에 의해 취득된 상기 콘텐츠 키를 이용하여, 상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠를 복호하는 복호 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는 증명서를 검출하는 증명서 검출 단계와,

상기 증명서 검출 단계의 처리에 의해 검출된 상기 증명서를, 인증국의 공개 키를 이용하여 검증하는 제1 검증 단계와,

상기 증명서 검출 단계의 처리에 의해 검출된 상기 증명서로부터, 상기 콘텐츠 제공자의 공개 키를 취득하는 공개 키 취득 단계와,

상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는 디지털 서명을 검출하는 디지털 서명 검출 단계와,

상기 디지털 서명 검출 단계의 처리에 의해 검출된 상기 디지털 서명을, 상기 공개 키 취득 단계의 처리에 의해 취득된 상기 콘텐츠 제공자의 상기 공개 키를 이용하여 검증하는 제2 검증 단계와,

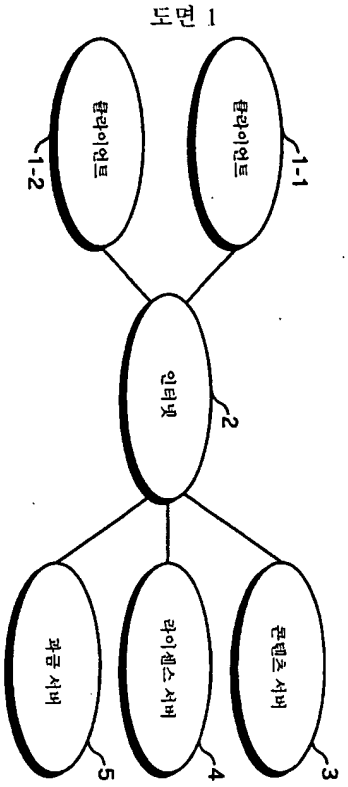
상기 콘텐츠 취득 단계의 처리에 의해 취득된 상기 콘텐츠에 부가되어 있는 헤더로부터, 워터마크를 검출하는 워터마크 검출 단계와,

상기 워터마크 검출 단계의 처리에 의해 검출된 상기 워터마크에 기초하여, 상기 콘텐츠의 출력을 제어하는 제어 단계

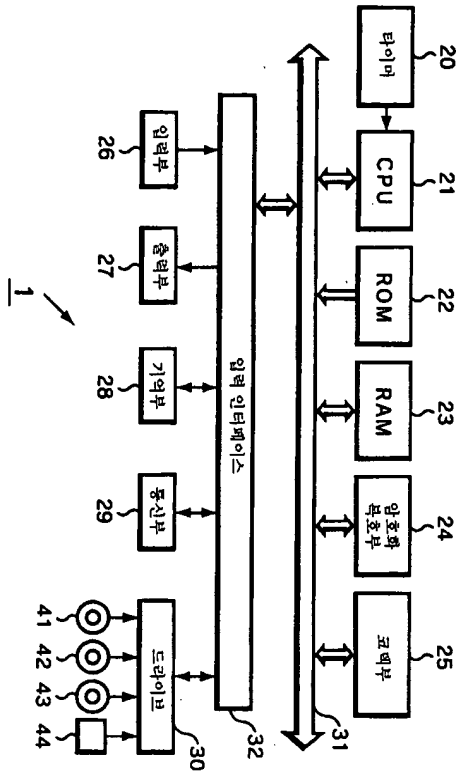
를 포함하는 것을 특징으로 하는 프로그램.

도면

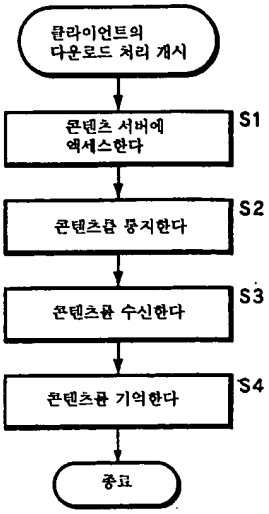
도면 1



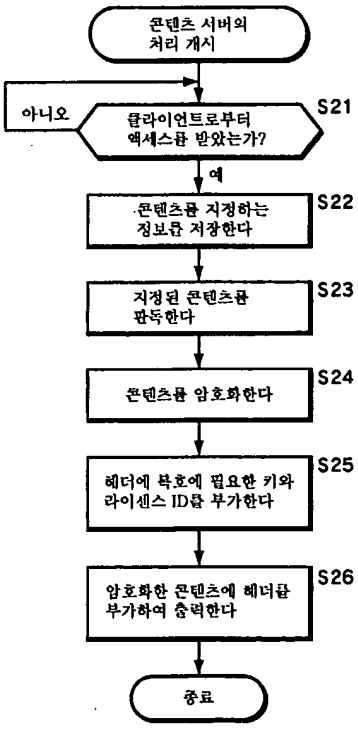
도면 2


1
타이머
20
CPU
21
ROM
22
RAM
23
암호화 복호부
24
코덱부
25
입력부
26
출력부
27
기억부
28
통신부
29
드라이브
30
31
입력 인터페이스
32
41
42
43
44

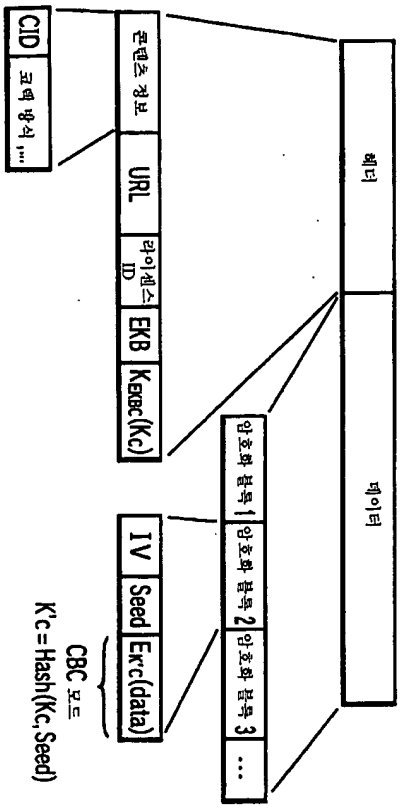
도면 3


클라이언트의
다운로드 처리 개시
콘텐츠 서버에
액세스한다
S1
콘텐츠를 문지한다
S2
콘텐츠를 수신한다
S3
콘텐츠를 기억한다
S4
종료

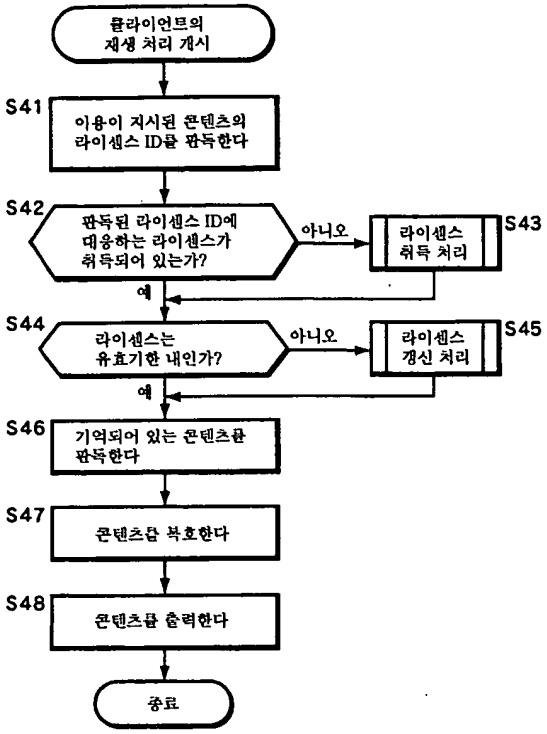
도면 4


콘텐츠 서버의
처리 개시
아니오
클라이언트로부터
액세스를 받았는가?
S21
예
콘텐츠를 지정하는
정보를 저장한다
S22
지정된 콘텐츠를
판독한다
S23
콘텐츠를 암호화한다
S24
헤더에 복호에 필요한 키와
라이센스 ID를 부가한다
S25
암호화한 콘텐츠에 헤더를
부가하여 출력한다
S26
종료

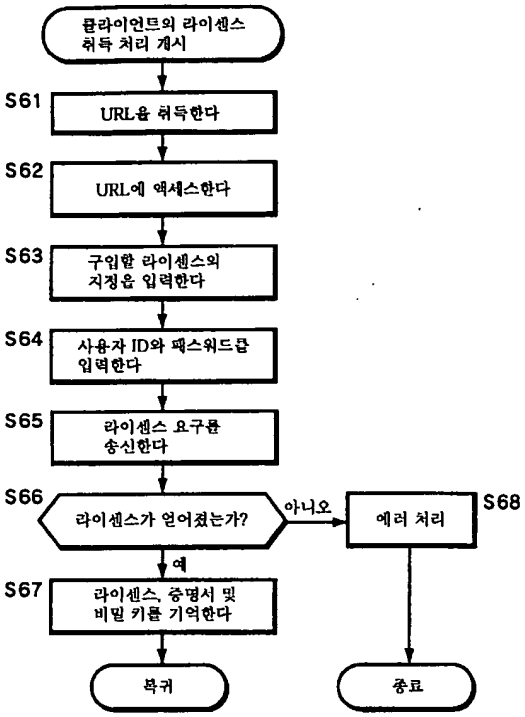
도면 5


헤더
데이터
콘텐츠 정보
URL
라이센스 ID
EKB
KEKBC(Kc)
CID
코덱 방식 ,...
암호화 블록 1
암호화 블록 2
암호화 블록 3
...
IV
Seed
EK'c(data)
CBC 모드
K'c=Hash(Kc,Seed)

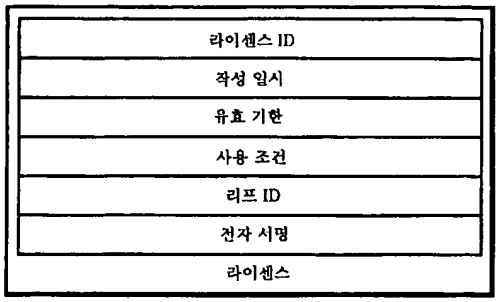
도면 6


클라이언트의
재생 처리 개시
S41
이용이 지시된 콘텐츠의
라이센스 ID를 판독한다
S42
판독된 라이센스 ID에
대응하는 라이센스가
취득되어 있는가?
아니오
라이센스
취득 처리
S43
예
S44
라이센스는
유효기한 내인가?
아니오
라이센스
갱신 처리
S45
예
S46
기억되어 있는 콘텐츠를
판독한다
S47
콘텐츠를 복호한다
S48
콘텐츠를 출력한다
종료

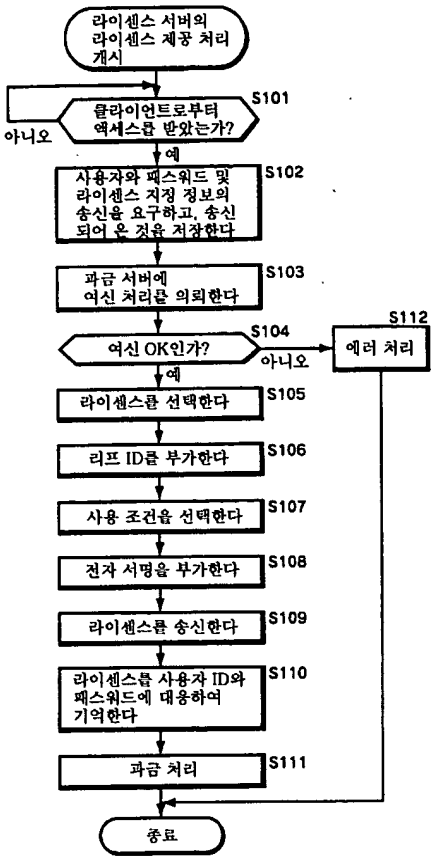
도면 7


클라이언트의 라이센스 취득 처리 개시
S61
URL을 취득한다
S62
URL에 액세스한다
S63
구입할 라이센스의 지정을 입력한다
S64
사용자 ID와 패스워드를 입력한다
S65
라이센스 요구를 송신한다
S66
라이센스가 얻어졌는가?
아니오
에러 처리
S68
예
S67
라이센스, 증명서 및 비밀 키를 기억한다
복귀
종료

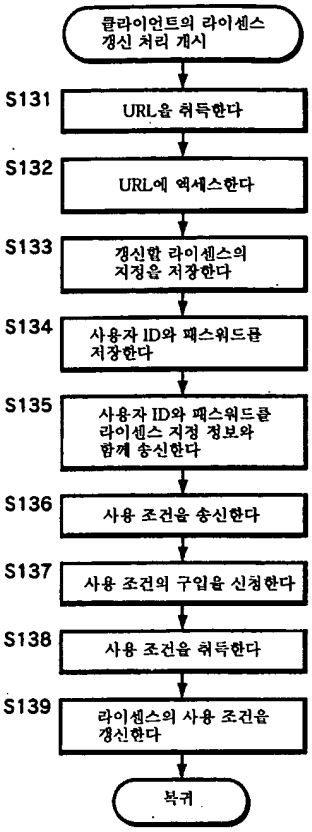
도면 8


라이센스 ID
작성 일시
유효 기한
사용 조건
리프 ID
전자 서명
라이센스

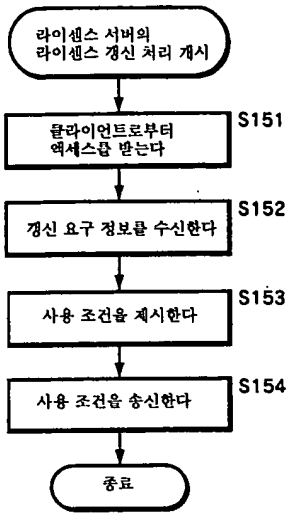
도면 9


라이센스 서버의
라이센스 제공 처리
개시
S101
클라이언트로부터
액세스를 받았는가?
아니오
예
S102
사용자와 패스워드 및
라이센스 지정 정보의
송신을 요구하고, 송신
되어 온 것을 저장한다
S103
과금 서버에
여신 처리를 의뢰한다
S104
여신 OK인가?
아니오
S112
에러 처리
예
S105
라이센스를 선택한다
S106
리프 ID를 부가한다
S107
사용 조건을 선택한다
S108
전자 서명을 부가한다
S109
라이센스를 송신한다
S110
라이센스를 사용자 ID와
패스워드에 대응하여
기억한다
S111
과금 처리
종료

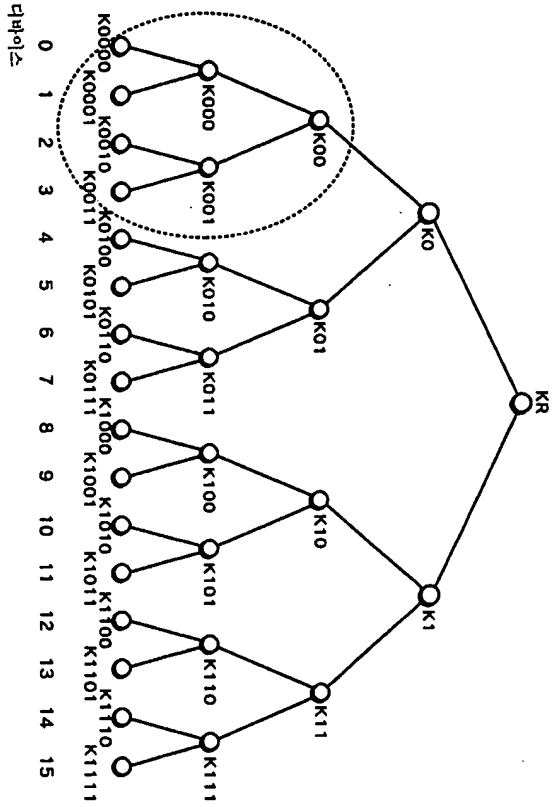
도면 10


클라이언트의 라이센스 갱신 처리 개시
S131
URL을 취득한다
S132
URL에 액세스한다
S133
갱신할 라이센스의 지정을 저장한다
S134
사용자 ID와 패스워드를 저장한다
S135
사용자 ID와 패스워드를 라이센스 지정 정보와 함께 송신한다
S136
사용 조건을 송신한다
S137
사용 조건의 구입을 신청한다
S138
사용 조건을 취득한다
S139
라이센스의 사용 조건을 갱신한다
복귀

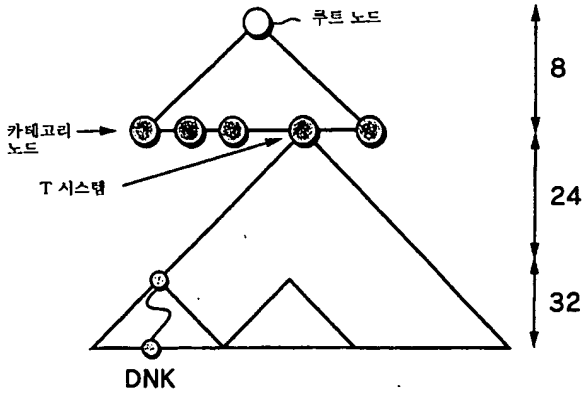
도면 11


라이센스 서버의
라이센스 갱신 처리 개시
클라이언트로부터
액세스를 받는다
S151
갱신 요구 정보를 수신한다
S152
사용 조건을 제시한다
S153
사용 조건을 송신한다
S154
종료

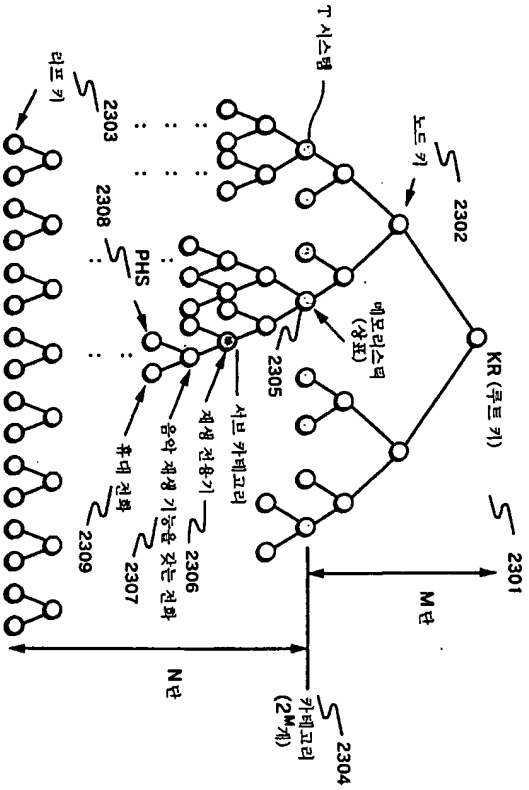
도면 12


디비이스
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
K000
K001
K010
K011
K100
K101
K110
K111
K00
K01
K10
K11
K0
K1
KR

도면 13


루트 노드
카테고리 노드
T 시스템
DNK
8
24
32

도면 14



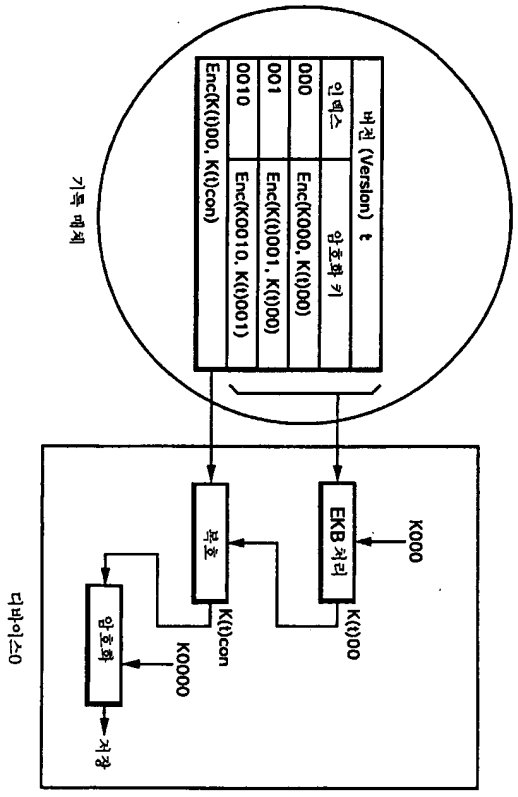
도면 15A

버전 (Version) t	
인덱스	암호화 키
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

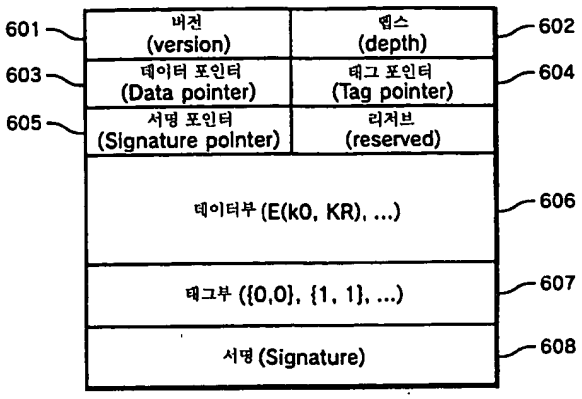
도면 15B

버전 (Version) t	
인덱스	암호화 키
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

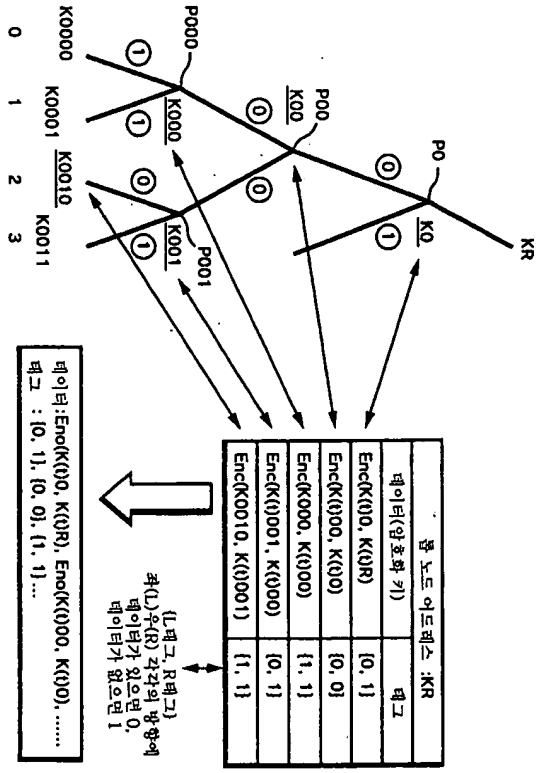
도면 16



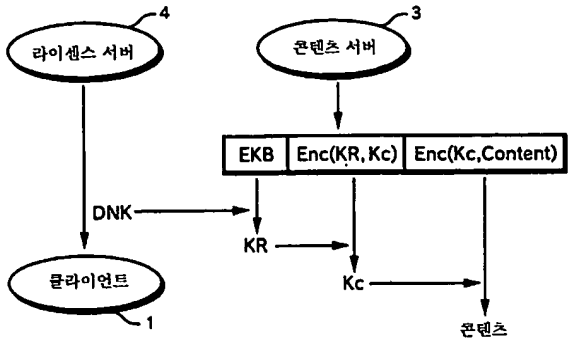
도면 17


601
버전 (version)
뎁스 (depth)
602
603
데이터 포인터 (Data pointer)
태그 포인터 (Tag pointer)
604
605
서명 포인터 (Signature pointer)
리저브 (reserved)
데이터부 (E(k0, KR), ...)
606
태그부 ({0,0}, {1, 1}, ...)
607
서명 (Signature)
608

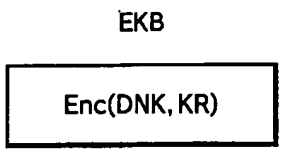
도면 18


K0000
K0001
K0010
K0011
P000
K000
P001
K001
P00
K00
P0
K0
KR
데이터:Enc(K(t)0, K(t)R), Enc(K(t)00, K(t)0), ... 태그 : {0, 1}, {0, 0}, {1, 1}....
{L태그, R태그}
좌(L)우(R) 각각의 방향에 데이터가 있으면 0, 데이터가 없으면 1
Enc(K0010, K(t)001)
Enc(K(t)001, K(t)000)
Enc(K000, K(t)00)
Enc(K(t)00, K(t)0)
Enc(K(t)0, K(t)R)
데이터(암호화 키)
{1, 1}
{0, 1}
{1, 1}
{0, 0}
{0, 1}
태그
루트 노드 어드레스 :KR

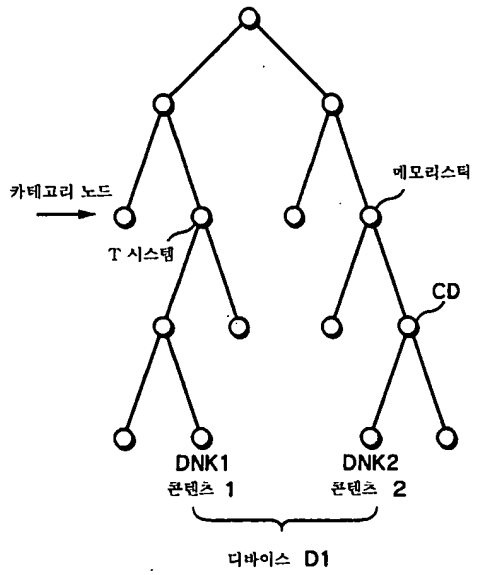
도면 19



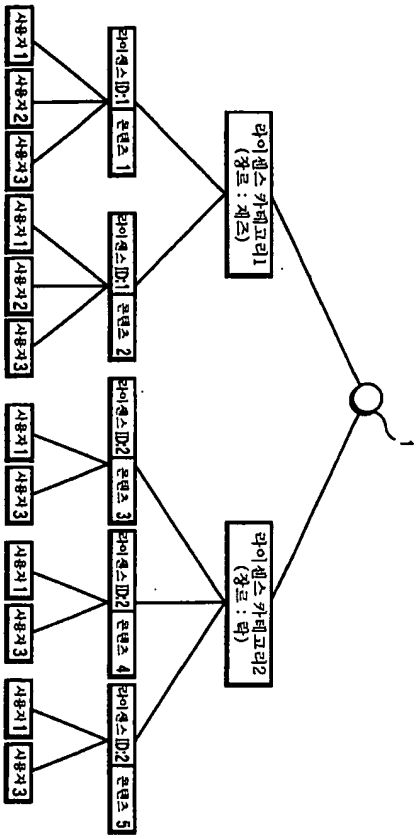
도면 20



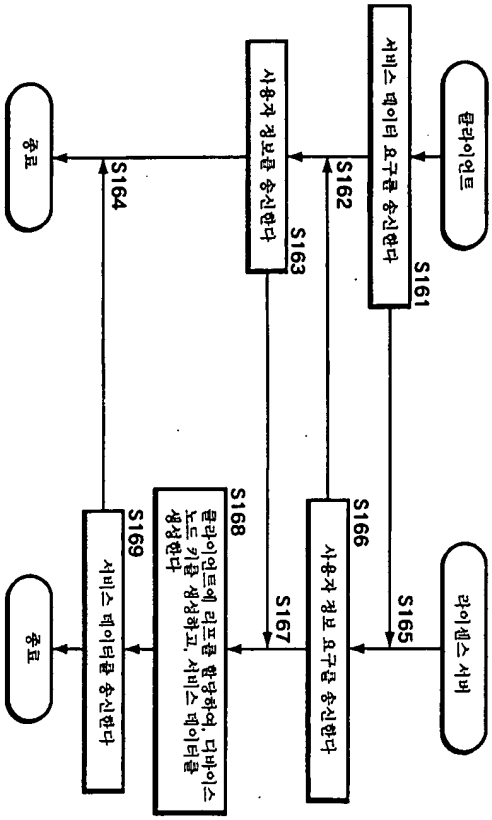
도면 21



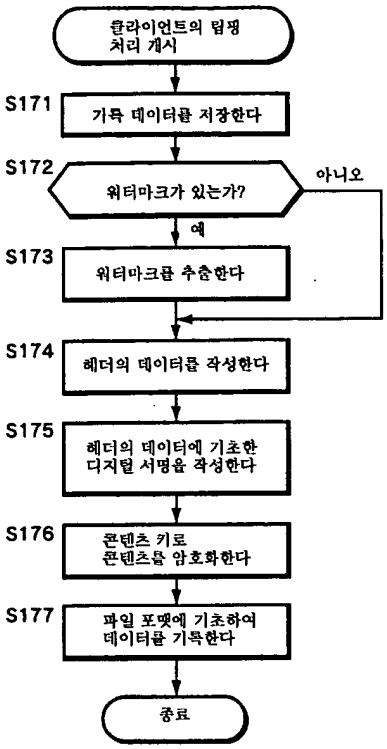
도면 22


라이센스 카테고리1
(장르 : 재즈)
라이센스 카테고리2
(장르 : 팝)
라이센스ID:1
로테츠 1
라이센스ID:1
로테츠 2
라이센스ID2
로테츠 3
라이센스ID2
로테츠 4
라이센스ID2
로테츠 5
사용자1
사용자2
사용자3
사용자1
사용자2
사용자3
사용자1
사용자3
사용자1
사용자3
사용자1
사용자3

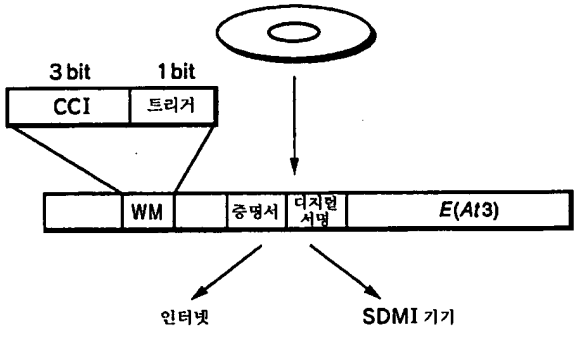
도면 23


클라이언트
서비스 데이터 요구를 송신한다
S161
S162
사용자 정보를 송신한다
S163
종료
S164
라이센스 서버
사용자 정보 요구를 송신한다
S166
S165
S167
클라이언트에 라프를 할당하여, 디바이스 노드 키를 생성하고, 서비스 데이터를 생성한다
S168
서비스 데이터를 송신한다
S169
종료

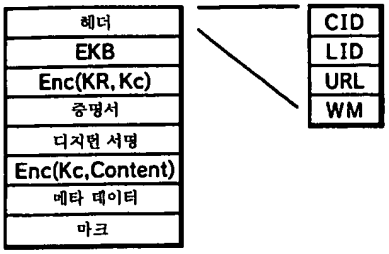
도면 24


클라이언트의 팀핑 처리 개시
S171
기록 데이터를 저장한다
S172
워터마크가 있는가?
아니오
예
S173
워터마크를 추출한다
S174
헤더의 데이터를 작성한다
S175
헤더의 데이터에 기초한 디지털 서명을 작성한다
S176
콘텐츠 키로 콘텐츠를 암호화한다
S177
파일 포맷에 기초하여 데이터를 기록한다
종료

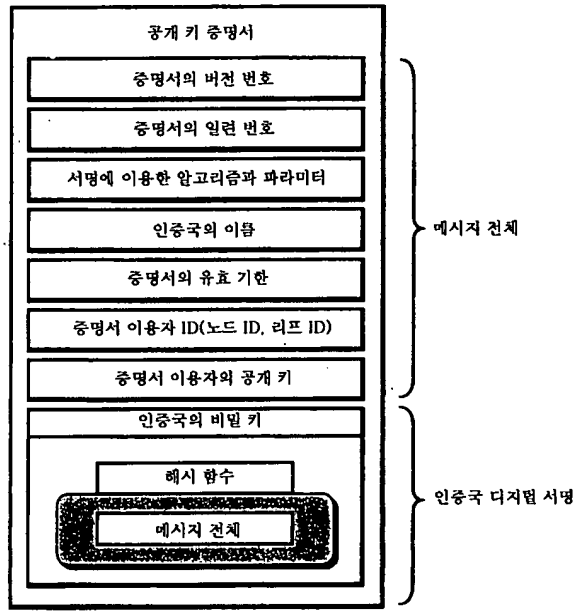
도면 25


3 bit
1 bit
CCI
트리거
WM
증명서
디지털 서명
E(At3)
인터넷
SDMI 기기

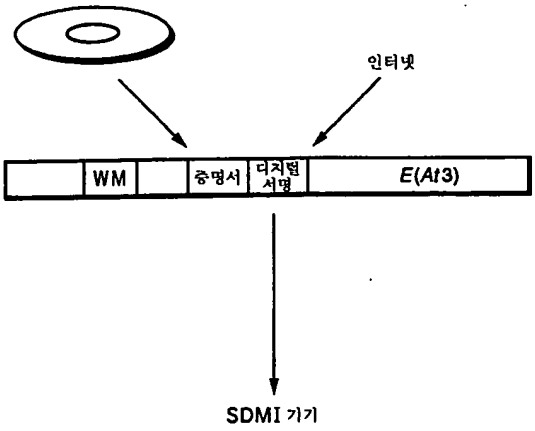
도면 26


헤더
EKB
Enc(KR, Kc)
증명서
디지털 서명
Enc(Kc,Content)
메타 데이터
마크
CID
LID
URL
WM

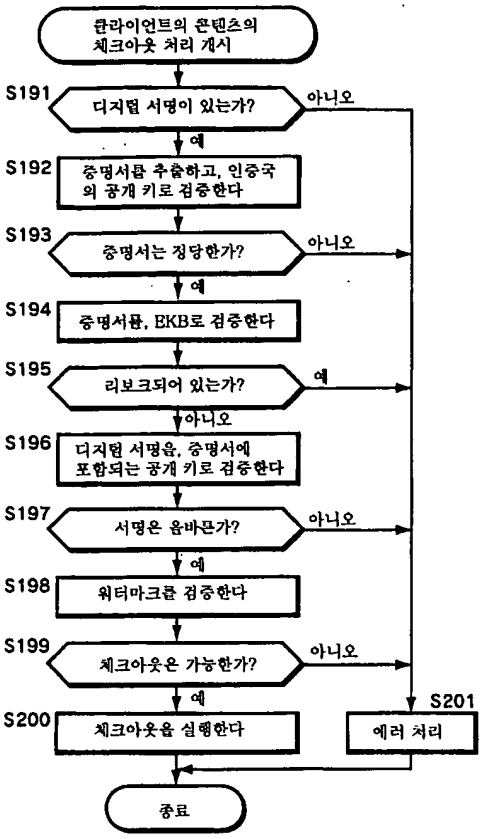
도면 27


공개 키 증명서
증명서의 버전 번호
증명서의 일련 번호
서명에 이용한 알고리즘과 파라미터
인증국의 이름
증명서의 유효 기한
증명서 이용자 ID(노드 ID, 리프 ID)
증명서 이용자의 공개 키
인증국의 비밀 키
해시 함수
메시지 전체
메시지 전체
인증국 디지털 서명

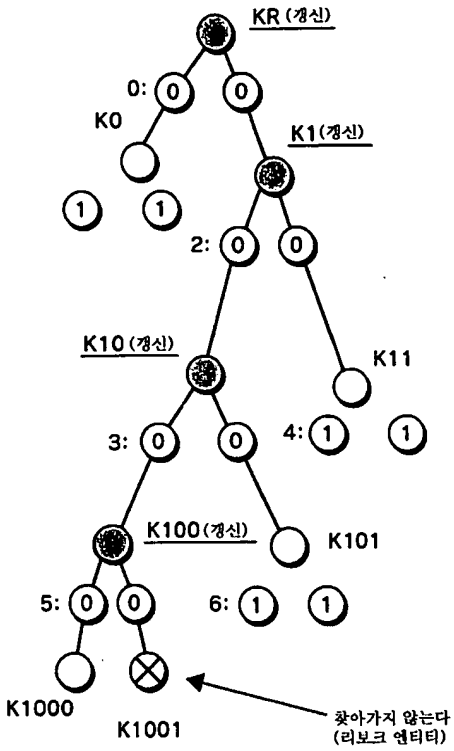
도면 28



도면 29


클라이언트의 콘텐츠의 체크아웃 처리 개시
S191
디지털 서명이 있는가?
아니오
예
S192
증명서를 추출하고, 인증국의 공개 키로 검증한다
S193
증명서는 정당한가?
아니오
예
S194
증명서를, EKB로 검증한다
S195
리보크되어 있는가?
예
아니오
S196
디지털 서명을, 증명서에 포함되는 공개 키로 검증한다
S197
서명은 올바른가?
아니오
예
S198
워터마크를 검증한다
S199
체크아웃은 가능한가?
아니오
예
S200
체크아웃을 실행한다
S201
에러 처리
종료

도면 30

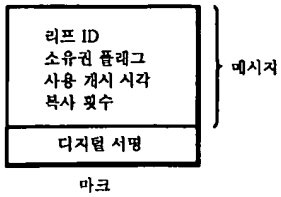


도면 31

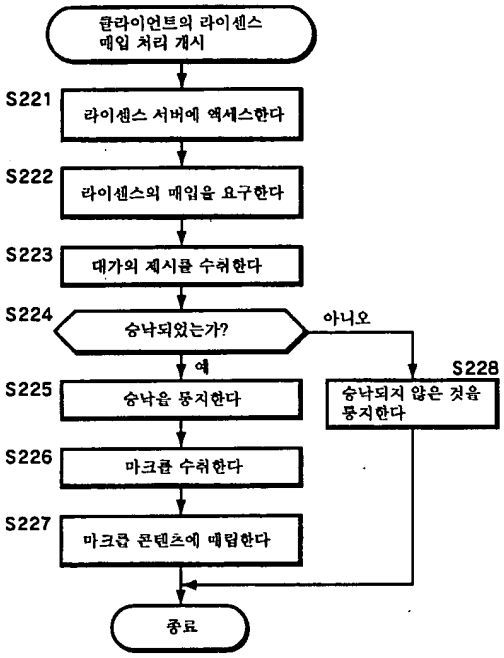
데이터 (암호화 키)	Enc(K0, K(t)R), Enc(K(t)1, K(t)R) Enc(K(t)10, K(t)1), Enc(K11, K(t)1) Enc(K(t)100, K(t)10), Enc(K101, K(t)10) Enc(K1000, K(t)100)
태그	0: {0, 0}, 1:{1, 1}, 2:{0, 0}, 3:(0, 0) 4: {1, 1}, 5:{0, 1}, 6:{1, 1}

{L태그, R태그}
좌(L)우(R) 각각의 방향에
데이터가 있으면 0, 데이터가 없으면 1

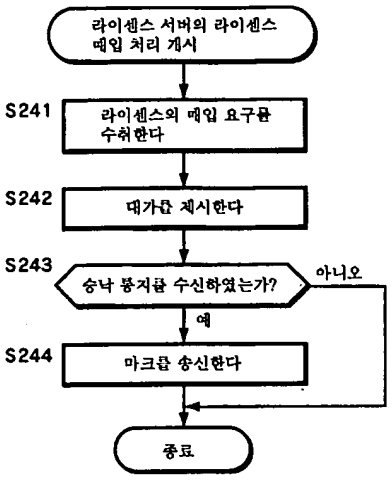
도면 32


리프 ID
소유권 플래그
사용 개시 시각
복사 횟수
메시지
디지털 서명
마크

도면 33

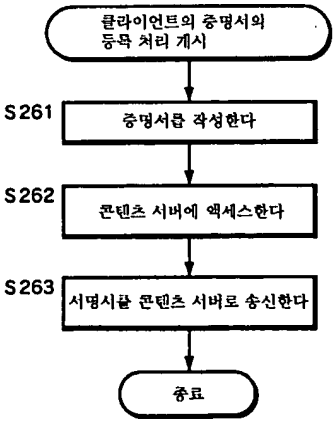

클라이언트의 라이센스
매입 처리 개시
S221
라이센스 서버에 액세스한다
S222
라이센스의 매입을 요구한다
S223
대가의 제시를 수취한다
S224
승낙되었는가?
아니오
예
S225
승낙을 통지한다
S228
승낙되지 않은 것을
통지한다
S226
마크를 수취한다
S227
마크를 콘텐츠에 매립한다
종료

도면 34

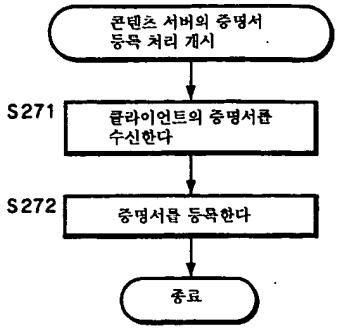


도면 35

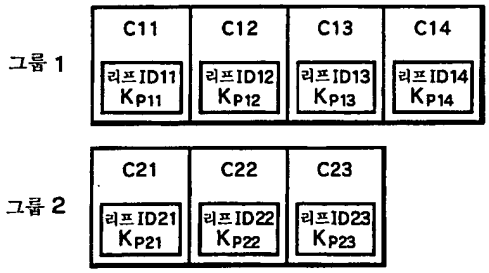
도면 36



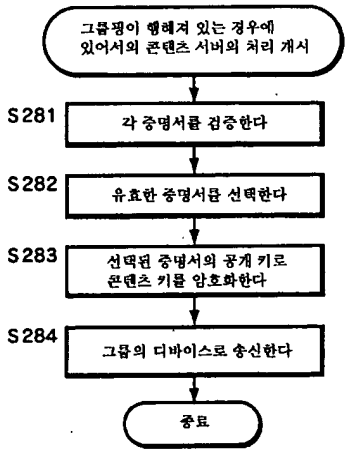
도면 37



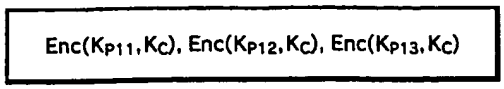
도면 38



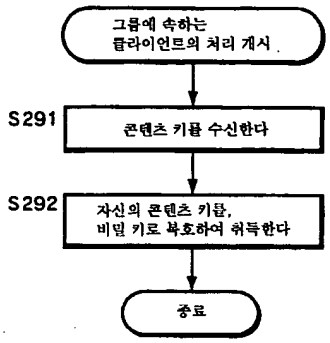
도면 39



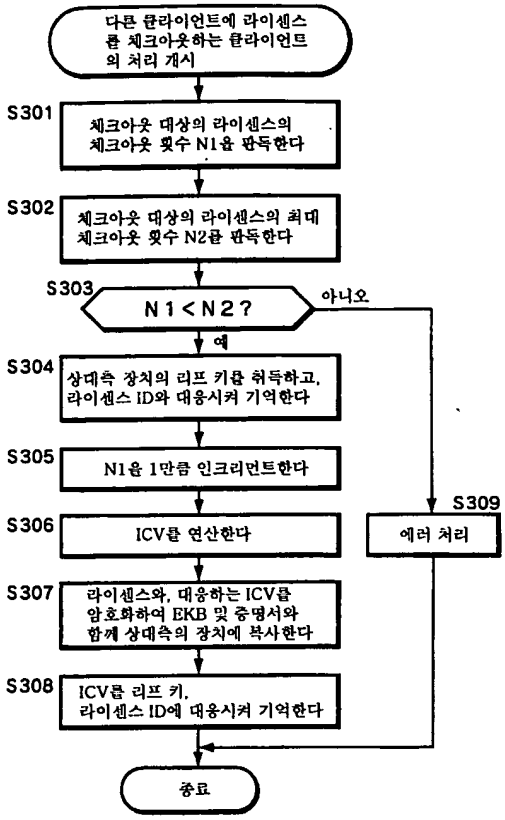
도면 40


Enc(KP11, KC), Enc(KP12, KC), Enc(KP13, KC)

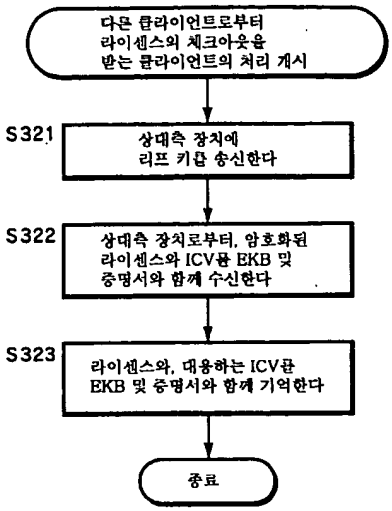
도면 41


그룹에 속하는
클라이언트의 처리 개시
S291
콘텐츠 키를 수신한다
S292
자신의 콘텐츠 키를,
비밀 키로 복호하여 취득한다
종료

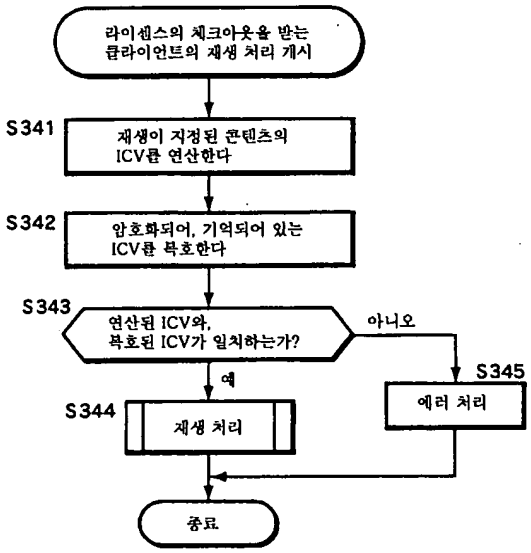
도면 42


다른 클라이언트에 라이센스를 체크아웃하는 클라이언트의 처리 개시
S301
체크아웃 대상의 라이센스의 체크아웃 횟수 N1을 판독한다
S302
체크아웃 대상의 라이센스의 최대 체크아웃 횟수 N2를 판독한다
S303
N1<N2?
아니오
예
S304
상대측 장치의 리프 키를 취득하고, 라이센스 ID와 대응시켜 기억한다
S305
N1을 1만큼 인크리먼트한다
S306
ICV를 연산한다
S307
라이센스와, 대응하는 ICV를 암호화하여 EKB 및 증명서와 함께 상대측의 장치에 복사한다
S308
ICV를 리프 키, 라이센스 ID에 대응시켜 기억한다
S309
에러 처리
종료

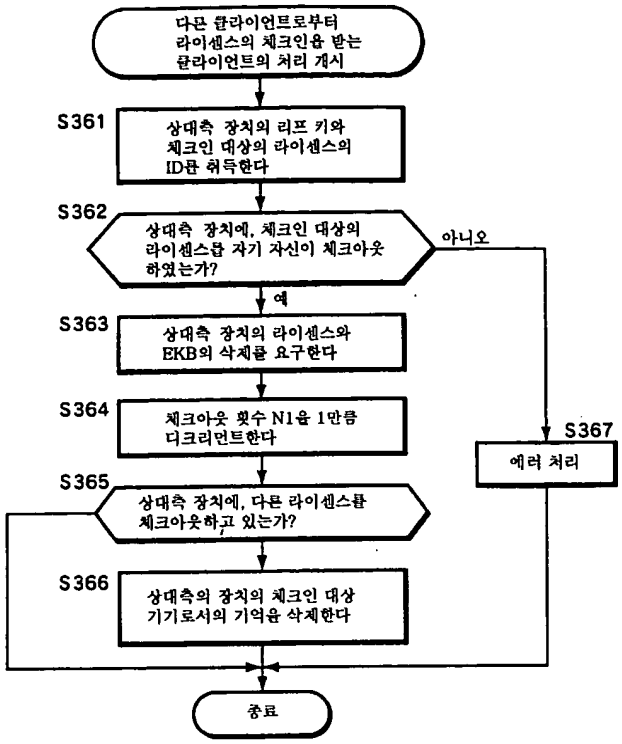
도면 43


다른 클라이언트로부터
라이센스의 체크아웃을
받는 클라이언트의 처리 개시
S321
상대측 장치에
리프 키를 송신한다
S322
상대측 장치로부터, 암호화된
라이센스와 ICV를 EKB 및
증명서와 함께 수신한다
S323
라이센스와, 대응하는 ICV를
EKB 및 증명서와 함께 기억한다
종료

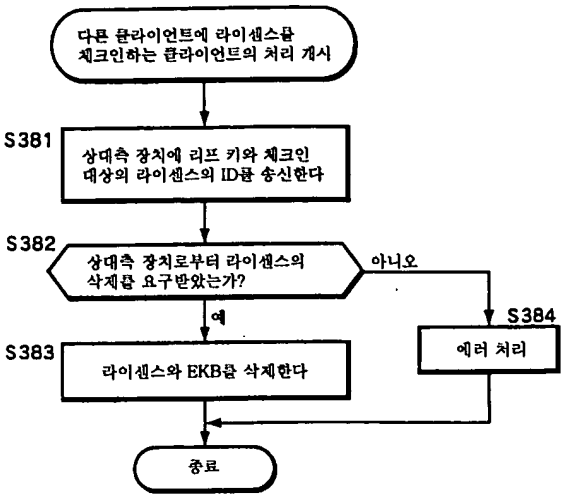
도면 44


라이센스의 체크아웃을 받는
클라이언트의 재생 처리 개시
S341
재생이 지정된 콘텐츠의
ICV를 연산한다
S342
암호화되어, 기억되어 있는
ICV를 복호한다
S343
연산된 ICV와,
복호된 ICV가 일치하는가?
아니오
예
S345
에러 처리
S344
재생 처리
종료

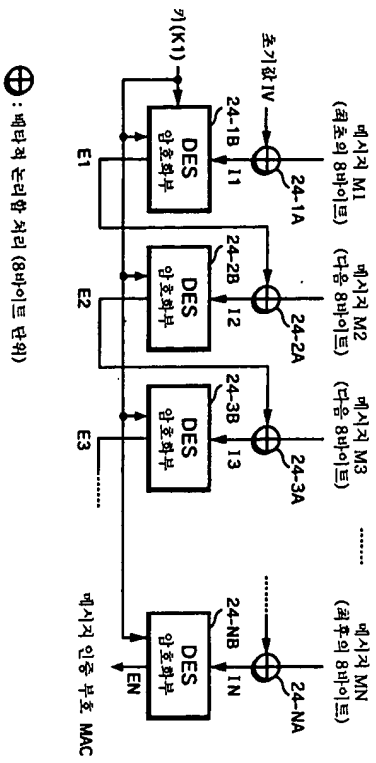
도면 45


다른 클라이언트로부터
라이센스의 체크인을 받는
클라이언트의 처리 개시
S361
상대측 장치의 리프 키와
체크인 대상의 라이센스의
ID를 취득한다
S362
상대측 장치에, 체크인 대상의
라이센스를 자기 자신이 체크아웃
하였는가?
아니오
예
S363
상대측 장치의 라이센스와
EKB의 삭제를 요구한다
S364
체크아웃 횟수 N1을 1만큼
디크리먼트한다
S365
상대측 장치에, 다른 라이센스를
체크아웃하고 있는가?
S366
상대측의 장치의 체크인 대상
기기로서의 기억을 삭제한다
S367
에러 처리
종료

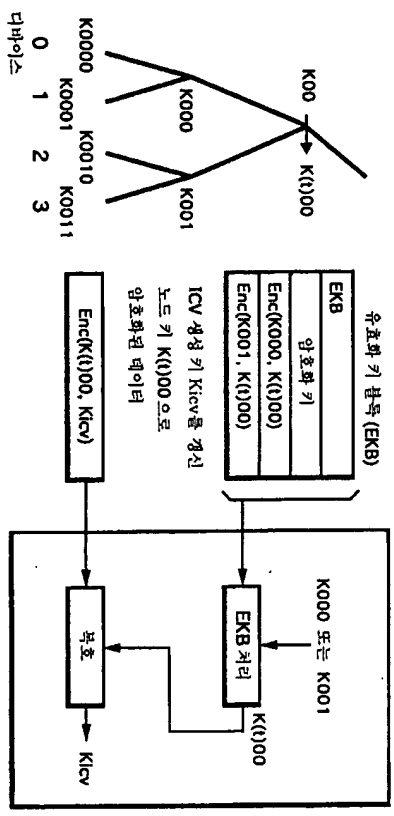
도면 46


다른 클라이언트에 라이센스를 체크인하는 클라이언트의 처리 개시
S381
상대측 장치에 리프 키와 체크인 대상의 라이센스의 ID를 송신한다
S382
상대측 장치로부터 라이센스의 삭제를 요구받았는가?
아니오
예
S384
에러 처리
S383
라이센스와 EKB를 삭제한다
종료

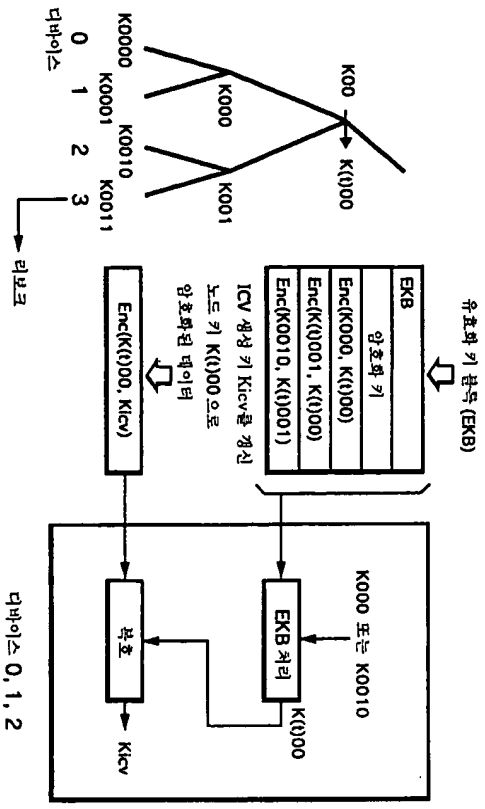
도면 47


메시지 M1
(최초의 8바이트)
메시지 M2
(다음 8바이트)
메시지 M3
(다음 8바이트)
메시지 MN
(최후의 8바이트)
초기값IV
키(K1)
24-1A
24-2A
24-3A
24-NA
24-1B
24-2B
24-3B
24-NB
DES
암호화부
I1
I2
I3
IN
E1
E2
E3
EN
메시지 인증 부호 MAC
⊕ : 베타적 논리합 처리 (8바이트 단위)

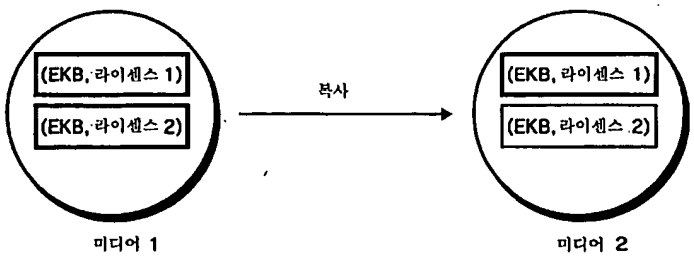
도면 48


디바이스
0
1
2
3
K0000
K0001
K0010
K0011
K000
K001
K00
K(t)00
유효화 키 블록 (EKB)
EKB
암호화 키
Enc(K000, K(t)00)
Enc(K001, K(t)00)
ICV 생성 키 Kicv를 갱신
노드 키 K(t)00으로
암호화된 데이터
Enc(K(t)00, Kicv)
K000 또는 K001
EKB 처리
K(t)00
복호
Kicv
디바이스 0, 1, 2, 3

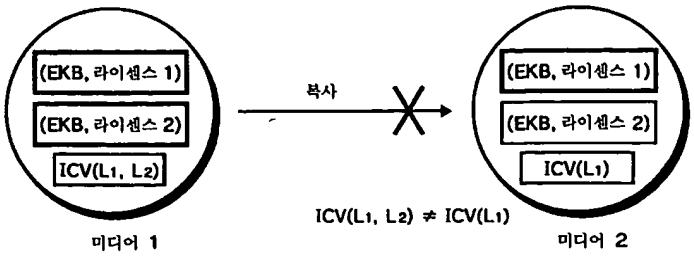
도면 49


디바이스
0
1
2
3
K0000
K0001
K0010
K0011
K000
K001
K00
K(i)00
리보크
Enc(K(i)00, Kicv)
ICV 생성 키 Kicv를 갱신
노드 키 K(i)00으로
암호화된 데이터
EKB
암호화 키
Enc(K000, K(i)00)
Enc(K(i)001, K(i)00)
Enc(K0010, K(i)001)
유효화 키 블록 (EKB)
디바이스 0, 1, 2
복호
EKB 처리
K000 또는 K0010
K(i)00
Kicv

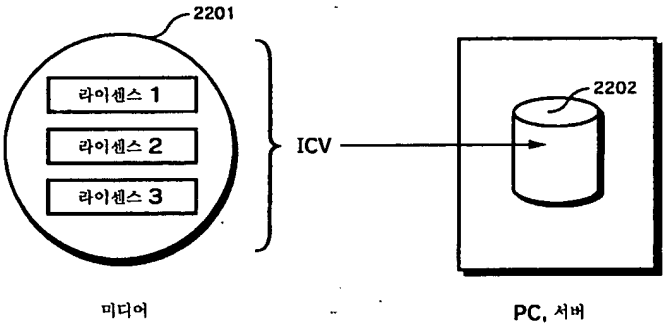
도면 50A


(EKB, 라이센스 1)
(EKB, 라이센스 2)
복사
(EKB, 라이센스 1)
(EKB, 라이센스 2)
미디어 1
미디어 2

도면 50B


(EKB, 라이센스 1)
(EKB, 라이센스 2)
ICV(L1, L2)
복사
(EKB, 라이센스 1)
(EKB, 라이센스 2)
ICV(L1)
ICV(L1, L2) ≠ ICV(L1)
미디어 1
미디어 2

도면 51


2201
라이센스 1
라이센스 2
라이센스 3
ICV
2202
미디어
PC, 서버